Center for Internet Security

CIS Benchmarks™

CIS Apple macOS 26 Tahoe Benchmark

v1.0.0 - 10-31-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Internal Only - General

Table of Contents

Terms of Use *1*

Table of Contents *2*

Overview *7*

Important Usage Information **7**

Key Stakeholders **7**

Apply the Correct Version of a Benchmark **8**

Exceptions **8**

Remediation **9**

Summary **9**

Target Technology Details **10**

Intended Audience **10**

Consensus Guidance **11**

Typographical Conventions **12**

Recommendation Definitions *13*

Title **13**

Assessment Status **13**

Automated **13**

Manual **13**

Profile **13**

Description **13**

Rationale Statement **13**

Impact Statement **14**

Audit Procedure **14**

Remediation Procedure **14**

Default Value **14**

References **14**

CIS Critical Security Controls® (CIS Controls®) **14**

Additional Information **14**

Profile Definitions **15**

Acknowledgements **16**

Recommendations *17*

1 Install Updates, Patches and Additional Security Software **17**

1.1 Ensure Apple-provided Software Updates Are Installed (Automated) 18

1.2 Ensure Download New Updates When Available Is Enabled (Automated) 23

1.3 Ensure Install of macOS Updates Is Enabled (Automated) 26

1.4 Ensure Install Application Updates from the App Store Is Enabled (Automated) 29

Internal Only - General

1.5 Ensure Install Security Responses and System Files Is Enabled (Automated) 32
1.6 Ensure Software Update Deferment Is Less Than or Equal to 30 Days (Automated)..... 36

2 System Settings..... 40
2.1 Apple Account 41
2.1.1 iCloud 42
2.1.1.1 Audit iCloud Passwords & Keychain (Manual)..... 43
2.1.1.2 Audit iCloud Drive (Manual) 46
2.1.1.3 Ensure iCloud Drive Document and Desktop Sync Is Disabled (Automated) 49
2.1.1.4 Audit Security Keys Used With Apple Accounts (Manual)..... 52
2.1.1.5 Audit Freeform Sync to iCloud (Manual)..... 54
2.1.1.6 Audit Find My Mac (Manual) 56
2.1.2 Audit App Store Password Settings (Manual)..... 60
2.2 Network..... 62
2.2.1 Ensure Firewall Is Enabled (Automated)..... 63
2.2.2 Ensure Firewall Stealth Mode Is Enabled (Automated) 66
2.3 General 69
2.3.1 AirDrop & Handoff..... 70
2.3.1.1 Ensure AirDrop Is Disabled When Not Actively Transferring Files (Automated)..... 71
2.3.1.2 Ensure AirPlay Receiver Is Disabled (Automated) 74
2.3.2 Date & Time 77
2.3.2.1 Ensure Set Time and Date Automatically Is Enabled (Automated) 78
2.3.2.2 Ensure the Time Service Is Enabled (Automated)..... 82
2.3.3 Sharing..... 84
2.3.3.1 Ensure Screen Sharing Is Disabled (Automated) 85
2.3.3.2 Ensure File Sharing Is Disabled (Automated)..... 88
2.3.3.3 Ensure Printer Sharing Is Disabled (Automated) 91
2.3.3.4 Ensure Remote Login Is Disabled (Automated)..... 93
2.3.3.5 Ensure Remote Management Is Disabled (Automated) 97
2.3.3.6 Ensure Remote Apple Events Is Disabled (Automated) 100
2.3.3.7 Ensure Internet Sharing Is Disabled (Automated) 102
2.3.3.8 Ensure Content Caching Is Disabled (Automated) 105
2.3.3.9 Ensure Media Sharing Is Disabled (Automated)..... 108
2.3.3.10 Ensure Bluetooth Sharing Is Disabled (Automated) 111
2.3.3.11 Ensure Computer Name Does Not Contain PII or Protected Organizational Information (Manual) 114
2.3.4 Time Machine 117
2.3.4.1 Ensure Backup Automatically is Enabled If Time Machine Is Enabled (Automated) . 118
2.3.4.2 Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled (Automated)..... 122
2.3.5 Language & Region 125
2.4 Menu Bar 125
2.4.1 Audit Menu Bar and Control Center Icons (Manual)..... 126
2.5 Apple Intelligence & Siri 128
2.5.1 Apple Intelligence 129
2.5.1.1 Ensure External Intelligence Extensions Is Disabled (Automated)..... 130
2.5.1.2 Ensure Writing Tools Is Disabled (Automated) 133
2.5.1.3 Ensure Mail Summarization Is Disabled (Automated) 136
2.5.1.4 Ensure Notes Summarization Is Disabled (Automated)..... 139
2.5.2 Siri..... 142
2.5.2.1 Ensure Siri Is Disabled (Automated) 143
2.5.2.2 Ensure Listen for (Siri) Is Disabled (Manual) 146
2.6 Privacy & Security 149
2.6.1 Location Services 150
2.6.1.1 Ensure Location Services Is Enabled (Automated) 151

Internal Only - General

2.6.1.2 Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled (Automated) 155
2.6.1.3 Audit Location Services Access (Manual) 158
2.6.2 Full Disk Access 161
2.6.2.1 Audit Full Disk Access for Applications (Manual) 162
2.6.3 Analytics & Improvements 164
2.6.3.1 Ensure Share Mac Analytics Is Disabled (Automated) 165
2.6.3.2 Ensure Improve Siri & Dictation Is Disabled (Automated) 167
2.6.3.3 Ensure Improve Assistive Voice Features Is Disabled (Automated) 169
2.6.3.4 Ensure 'Share with app developers' Is Disabled (Automated) 171
2.6.3.5 Ensure Share iCloud Analytics Is Disabled (Manual) 173
2.6.4 Ensure Limit Ad Tracking Is Enabled (Automated) 175
2.6.5 Ensure Gatekeeper Is Enabled (Automated) 177
2.6.6 Ensure FileVault Is Enabled (Automated) 180
2.6.7 Audit Lockdown Mode (Manual) 183
2.6.8 Ensure an Administrator Password Is Required to Access System-Wide Preferences (Automated) 185
2.7 Desktop & Dock 189
2.7.1 Ensure Screen Saver Corners Are Secure (Automated) 190
2.7.2 Audit iPhone Mirroring (Manual) 192
2.8 Displays 194
2.8.1 Audit Universal Control Settings (Manual) 195
2.9 Spotlight 198
2.9.1 Ensure Help Apple Improve Search Is Disabled (Automated) 199
2.10 Battery (Energy Saver) 201
2.10.1 OS Resuming From Sleep 202
2.10.1.1 Ensure the OS Is Not Active When Resuming from Standby (Intel) (Manual) 203
2.10.1.2 Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices (Automated) 207
2.10.2 Ensure Power Nap Is Disabled for Intel Macs (Automated) 211
2.10.3 Ensure Wake for Network Access Is Disabled (Automated) 215
2.11 Lock Screen 220
2.11.1 Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled (Automated) 221
2.11.2 Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately (Automated) 223
2.11.3 Ensure a Custom Message for the Login Screen Is Enabled (Automated) 227
2.11.4 Ensure Login Window Displays as Name and Password Is Enabled (Automated) 230
2.11.5 Ensure Show Password Hints Is Disabled (Automated) 232
2.12 Touch ID & Password (Login Password) 235
2.12.1 Ensure Users' Accounts Do Not Have a Password Hint (Automated) 236
2.12.2 Audit Touch ID (Manual) 238
2.13 Users & Groups 242
2.13.1 Ensure Guest Account Is Disabled (Automated) 243
2.13.2 Ensure Guest Access to Shared Folders Is Disabled (Automated) 246
2.13.3 Ensure Automatic Login Is Disabled (Automated) 248
2.14 Game Center 251
2.14.1 Audit Game Center Settings (Manual) 252
2.15 Notifications 255
2.15.1 Audit Notification Settings (Manual) 256
2.16 Wallet & Apple Pay 258
2.16.1 Audit Wallet & Apple Pay Settings (Manual) 259
2.17 Internet Accounts 261
2.17.1 Audit Internet Accounts for Authorized Use (Manual) 262
2.18 Keyboard 265
2.18.1 Ensure On-Device Dictation Is Enabled (Automated) 266

Internal Only - General

3 Logging and Auditing 268
3.1 Ensure Security Auditing Is Enabled (Automated) 269
3.2 Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements (Automated) 271
3.3 Ensure install.log Is Retained for 365 or More Days and No Maximum Size (Automated) 274
3.4 Ensure Security Auditing Retention Is Enabled (Automated) 276
3.5 Ensure Access to Audit Records Is Controlled (Automated) 278
3.6 Audit Software Inventory (Manual) 282

4 Network Configurations 284
4.1 Ensure Bonjour Advertising Services Is Disabled (Automated) 285
4.2 Ensure HTTP Server Is Disabled (Automated) 288
4.3 Ensure NFS Server Is Disabled (Automated) 290

5 System Access, Authentication and Authorization 292
5.1 File System Permissions and Access Controls 293
5.1.1 Ensure Home Folders Are Secure (Automated) 294
5.1.2 Ensure System Integrity Protection Status (SIP) Is Enabled (Automated) 297
5.1.3 Ensure Apple Mobile File Integrity (AMFI) Is Enabled (Automated) 300
5.1.4 Ensure Signed System Volume (SSV) Is Enabled (Automated) 302
5.1.5 Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated) 304
5.1.6 Ensure No World Writable Folders Exist in the System Folder (Automated) 306
5.1.7 Ensure No World Writable Folders Exist in the Library Folder (Automated) 308
5.2 Account and Password Policy Management 310
5.2.1 Ensure Password Account Lockout Threshold Is Configured (Automated) 312
5.2.2 Ensure Password Minimum Length Is Configured (Automated) 314
5.2.3 Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Manual) 316
5.2.4 Ensure Complex Password Must Contain Numeric Character Is Configured (Manual) 318
5.2.5 Ensure Complex Password Must Contain Special Character Is Configured (Manual) ..320
5.2.6 Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Manual) 322
5.2.7 Ensure Password Age Is Configured (Automated) 324
5.2.8 Ensure Password History Is Set to at least 24 (Automated) 326
5.3 Encryption 328
5.3.1 Ensure all user storage APFS volumes are encrypted (Manual) 329
5.3.2 Ensure all user storage CoreStorage volumes are encrypted (Manual) 333
5.4 Ensure the Sudo Timeout Period Is Set to Zero (Automated) 337
5.5 Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated) 339
5.6 Ensure the "root" Account Is Disabled (Automated) 342
5.7 Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session (Automated) 345
5.8 Ensure a Login Window Banner Exists (Automated) 348
5.9 Ensure the Guest Home Folder Does Not Exist (Automated) 351
5.10 Ensure XProtect Is Running and Updated (Automated) 353
5.11 Ensure Logging Is Enabled for Sudo (Automated) 356

6 Applications 358
6.1 Finder 359
6.1.1 Audit Show All Filename Extensions (Manual) 360
6.2 Mail 363
6.2.1 Ensure Protect Mail Activity in Mail Is Enabled (Manual) 364
6.3 Safari 366
6.3.1 Ensure Automatic Opening of Safe Files in Safari Is Disabled (Automated) 367
6.3.2 Audit History and Remove History Items (Manual) 369

Internal Only - General

6.3.3 Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled (Automated) ..371
6.3.4 Ensure Prevent Cross-site Tracking in Safari Is Enabled (Automated) ..373
6.3.5 Audit Hide IP Address in Safari Setting (Manual) ..376
6.3.6 Ensure Advertising Privacy Protection in Safari Is Enabled (Automated) ..380
6.3.7 Ensure Show Full Website Address in Safari Is Enabled (Automated) ..382
6.3.8 Audit AutoFill (Manual) ..384
6.3.9 Audit Pop-up Windows (Manual) ..386
6.3.10 Ensure Show Status Bar Is Enabled (Automated) ..388
6.4 Terminal ..390
6.4.1 Ensure Secure Keyboard Entry Terminal.app Is Enabled (Automated) ..391
6.5 Passwords ..393
6.5.1 Audit Passwords (Manual) ..394
7 Supplemental ..397
7.1 CIS Apple macOS Benchmark development collaboration with mSCP ..398
7.2 Apple Push Notification Service (APNs) ..399
7.3 Mobile Configuration Profiles ..400
7.4 Mobile Device Management (MDM) Software ..401
Appendix: Summary Table ..403
Appendix: CIS Controls v7 IG 1 Mapped Recommendations ..413
Appendix: CIS Controls v7 IG 2 Mapped Recommendations ..418
Appendix: CIS Controls v7 IG 3 Mapped Recommendations ..423
Appendix: CIS Controls v7 Unmapped Recommendations ..428
Appendix: CIS Controls v8 IG 1 Mapped Recommendations ..429
Appendix: CIS Controls v8 IG 2 Mapped Recommendations ..434
Appendix: CIS Controls v8 IG 3 Mapped Recommendations ..439
Appendix: CIS Controls v8 Unmapped Recommendations ..444
Appendix: Change History ..445

Internal Only - General

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Internal Only - General

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Internal Only - General

Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completes successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Internal Only - General

Target Technology Details

This document, CIS Apple macOS 26 Tahoe Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Apple macOS 26 Tahoe. This guide was tested against Apple macOS 26 Tahoe. To obtain the latest version of this guide, please visit https://www.cisecurity.org/cis-benchmarks/. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

This Benchmark includes instructions for auditing and remediation containing three different methods: Graphical User Interface (GUI), Command Line Interface using Terminal (CLI), and Configuration Profiles. These may be used to evaluate current configuration status and make changes as desired. In most cases, all methods are supported by the Operating System and it is up to organizational implementation personnel on how best to implement. There are some recommendations that can only be managed through one of these methods. Each organization must decide if control management outside their standard process is required if no solution is possible through their organization's specific choice of implementation. It is best practice at this time for Enterprise-managed devices to use profiles for management. A mix of both profile device management and command line hardening scripts will be the most comprehensive solution.

With the functionality of mobile configuration profiles, there has been an update to several recommendations. Any recommendation that is user specific but has a profile that sets a system-wide setting are compliant only with the profile installed. Any user specific settings have been moved to the Additional Information section but will no longer pass the audit.

More profile information

https://developer.apple.com/documentation/devicemanagement

https://developer.apple.com/documentation/devicemanagement/configuring-multiple-devices-using-profiles

Organizations that are using profiles should remember that a profile can limit what, if any, settings can be changed based on the profile payload. Even authorized organization technical personnel may not be able to change a setting with a profile in place. If technical personnel are expected to make changes that are contrary to profile settings, the profile may need to be reviewed in order to verify which accounts and what conditions apply, or a process to temporarily remove the profile should be in place.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Apple macOS 26 Tahoe.

Internal Only - General

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Internal Only - General

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Internal Only - General

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Internal Only - General

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Internal Only - General

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

Internal Only - General

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Ron Colvin, Ron Colvin

Contributor
William Harrison
Tim Harrison CISSP, ICP, KMP, Center for Internet Security, New York
Jason Olsen BSCS, Comerica Bank
Bob Gendler
Dan Brodjieski
Isaac Ordonez , Mann Consulting
Joe Goerlich , Siemens AG
Kari Byrd
John Mahlman
Matt Durante
Henry Stamerjohann
Michael Scarborough
Allen Golbig
Mischa van der Bent
Tony Young
Andrew Taylor

Editor
Edward Byrd , Center for Internet Security, New York

Internal Only - General

Recommendations

1 Install Updates, Patches and Additional Security Software

Good operational security involves timely remediation of known vulnerabilities. In order to reduce platform risk, updates need to be deployed in a timely manner.

CIS recognizes that most organizations require additional third party applications (security agents, connectivity solutions, productivity applications, etc.) in order to satisfy various organizational mandates. Such products should be carefully evaluated before implementation. CIS does not provide specific evaluation and/or compliance criteria for third party products. If organizations choose to implement third-party solutions, they should choose solutions that have demonstrated solid commitment to Apple platforms. Examples of such commitment include but are not limited to: timely support for new versions of macOS, native code base, and adherence to Apple Developer guidelines and best practices.

Internal Only - General

1.1 Ensure Apple-provided Software Updates Are Installed (Automated)

Profile Applicability:

- Level 1

Description:

Software vendors release security patches and software updates for their products when security vulnerabilities are discovered. There is no simple way to complete this action without a network connection to an Apple software repository. Please ensure appropriate access for this control. This check is only for what Apple provides through software update.

Rationale:

It is important that these updates be applied in a timely manner to prevent unauthorized persons from exploiting the identified vulnerabilities.

Impact:

Installation of updates can be disruptive to the users especially if a restart is required. Major updates need to be applied after creating an organizational patch policy. It is also advised to run updates and forced restarts during system downtime and not while in active use.

Internal Only - General

Audit:

Graphical Method:

Perform the following to ensure there are no available software updates:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select Show Updates to verify that there are no software updates available

Terminal Method:

Run the following command to verify there are no software updates currently available:

```
% /usr/bin/sudo /usr/bin/defaults read
/Library/Preferences/com.apple.SoftwareUpdate LastFullSuccessfulDate
```

The output will contain the date software update was last checked, ex `2025-09-05 13:28:46 +0000`, and must be within 30 days.

```
% /usr/bin/sudo /usr/bin/defaults read
/Library/Preferences/com.apple.SoftwareUpdate RecommendedUpdates
```

The output will show any updates awaiting to be installed, ex:

```
(
        {
            "Display Name" = "macOS Tahoe 26.0.1";
            "Display Version" = "26.0.1";
            Identifier = "MSU_UPDATE_25A362_patch_26.0.1_minor";
            MobileSoftwareUpdate = 1;
            "Product Key" = "MSU_UPDATE_25A362_patch_26.0.1_minor";
    }
)
```

Note: If you are running a previous version of macOS, the output will say that the current version is available. As long as the system is on the current point release of macOS, it is compliant. It is recommended that your organization moves to the current version of macOS once a .1 version is released. Be aware that old macOS versions will stop receiving any updates.

Note: Computers that have installed pre-release software in the past will fail this check if there are pre-release software updates available when audited.

Internal Only - General

Remediation:

Graphical Method:

Perform the following to install all available software updates:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select `Update All`

Terminal Method:

Run the following command to verify what packages need to be installed:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -l
```

The output will include the following: `Software Update found the following new or updated software:`

Note: If the software update server cannot be reached, that will need further investigation. This could be due to a network issue and must be resolved within your organization.

Run the following command to install all the packages that need to be updated:

To install all updates run the command:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -i -a
```

Or run the following command to install individual packages:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -i '<package name>'
```

Note: If one of the software updates listed includes `Action: restart`, then you must attach the `-R` flag to force a system restart. If the system update is complete but no restart occurs, then the system is in an unknown state that requires a future restart. It is advised to run updates and forced restarts during system downtime and not while in active use.

Internal Only - General

example:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -l

Software Update Tool

Finding available software
Software Update found the following new or updated software:
* Label: ProVideoFormats-2.2.7
        Title: Pro Video Formats, Version: 2.2.7, Size: 9693KiB, Recommended:
YES,
* Label: Command Line Tools for Xcode-15.0
        Title: Command Line Tools for Xcode, Version: 15.0, Size: 721962KiB,
Recommended: YES,

% /usr/bin/sudo /usr/sbin/softwareupdate -i 'ProVideoFormats-2.2.7'

Software Update Tool

Finding available software
Attempting to quit apps: (
    "com.apple.Compressor"
)
Waiting for user to quit any relevant apps
Successfully quit all apps

Downloaded Pro Video Formats
Installing Pro Video Formats
Done with Pro Video Formats
Done.
```

In the above example, if a restart was required, the command to remediate would be `/usr/bin/sudo /usr/sbin/softwareupdate -i 'ProVideoFormats-2.2.7' -R`

References:

1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Internal Only - General

Additional Information:

If software update has not been ran on the system previously (GUI or in Terminal), then the End User License agreement may need to be accepted when running `softwareupdate -i`. Where that is needed, include the `--agree-to-license` option.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

1.2 Ensure Download New Updates When Available Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

In the GUI, both "Install macOS updates" and "Install app updates from the App Store" are dependent on whether "Download new updates when available" is selected.

Rationale:

It is important that a system has the newest updates downloaded so that they can be applied.

Impact:

If "Download new updates when available" is not selected, updates may not be made in a timely manner and the system will be exposed to additional risk.

Audit:

Perform the following to ensure the system is automatically checking for updates:

Graphical Method:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Verify that `Download new updates when available` is enabled

Terminal Method:

Run the following command to verify that software updates are automatically checked:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticDownload').js
EOS

true
```

Note: If automatic updates were selected during system setup, this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

Internal Only - General

Remediation:

Perform the following to enable the system to automatically check for updates:

Graphical Method:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Set `Download new updates when available` to enabled
6. Select `Done`

Terminal Method:

Run the following command to enable auto update:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate AutomaticDownload -bool true
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.SoftwareUpdate`
2. The key to include is `AutomaticDownload`
3. The key must be set to `<true/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

1.3 Ensure Install of macOS Updates Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that macOS updates are installed after they are available from Apple. This setting enables macOS updates to be automatically installed. Some environments will want to approve and test updates before they are delivered. It is best practice to test first where updates can and have caused disruptions to operations. Automatic updates should be turned off where changes are tightly controlled and there are mature testing and approval processes. Automatic updates should not be turned off simply to allow the administrator to contact users in order to verify installation. A dependable, repeatable process involving a patch agent or remote management tool should be in place before auto-updates are turned off.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

Impact:

Unpatched software may be exploited.

Audit:

Graphical Method:

Perform the following to ensure that macOS updates are set to auto update:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Verify that `Install macOS updates` is enabled

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Automatically Install macOS Updates` set to `True`

Internal Only - General

Terminal Method:

Run the following command to verify that macOS updates are automatically checked and installed:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticallyInstallMacOSUpdates').js
EOS

true
```

Note: If automatic updates were selected during system setup, this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

Remediation:

Graphical Method:

Perform the following steps to enable macOS updates to run automatically:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Set `Install macOS updates` to enabled
6. Select `Done`

Terminal Method:

Run the following command to to enable automatic checking and installing of macOS updates:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate
AutomaticallyInstallMacOSUpdates -bool TRUE
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.SoftwareUpdate`
2. The key to include is `AutomaticallyInstallMacOSUpdates`
3. The key must be set to `<true/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

1.4 Ensure Install Application Updates from the App Store Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that application updates are installed after they are available from Apple. These updates do not require reboots or administrator privileges for end users.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

Impact:

Unpatched software may be exploited.

Audit:

Graphical Method:

Perform the following steps to ensure that App Store updates install automatically:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Verify that `Install application updates from the App Store` is enabled

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Automatically Install App Updates` set to `True`

Internal Only - General

Terminal Method:

Run the following command to verify that App Store updates are auto updating:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.commerce')\
  .objectForKey('AutoUpdate'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdat
e')\
  .objectForKey('AutomaticallyInstallAppUpdates'))
  if ( pref1 == 1 || pref2 == 1 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to enable App Store updates to install automatically:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Set `Install application updates from the App Store` to enabled
6. Select `Done`

Terminal Method:

Run the following command to turn on App Store auto updating:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.commerce AutoUpdate -bool TRUE
```

Note: This remediation requires a log out and log in to show in the GUI.

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.SoftwareUpdate`
2. The key to include is `AutomaticallyInstallAppUpdates`
3. The key must be set to `<true/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

1.5 Ensure Install Security Responses and System Files Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that system and security updates are installed after they are available from Apple. This setting enables definition updates for XProtect and Gatekeeper. With this setting in place, new malware and adware that Apple has added to the list of malware or untrusted software will not execute. These updates do not require reboots or end user admin rights.

Apple has introduced a security feature that allows for smaller downloads and the installation of security updates when a reboot is not required. This feature is only available when the last regular update has already been applied. This feature emphasizes that a Mac must be up-to-date on patches so that Apple's security tools can be used to quickly patch when a rapid response is necessary.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

Impact:

Unpatched software may be exploited.

Audit:

Graphical Method:

Perform the following steps to ensure that system data files and security updates install automatically:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Verify that `Install Security Responses and System files` is enabled

Internal Only - General

Terminal Method:

Run the following commands to verify that system data files and security updates are automatically checked:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdat
e')\
  .objectForKey('ConfigDataInstall'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdat
e')\
  .objectForKey('CriticalUpdateInstall'))
  if ( pref1 == 1 && pref2 == 1 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Note: If automatic updates were selected during system setup, this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

Remediation:

Graphical Method:

Perform the following steps to enable system data files and security updates to install automatically:

1. Open `System Settings`
2. Select `General`
3. Select `Software Update`
4. Select the `i`
5. Set `Install Security Responses and System files` to enabled
6. Select `Done`

Internal Only - General

Terminal Method:

Run the following commands to enable automatic checking of system data files and security updates:

```
% /usr/bin/sudo  /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate ConfigDataInstall -bool true

% /usr/bin/sudo  /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate CriticalUpdateInstall -bool
true
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.SoftwareUpdate`
2. The key to include is `ConfigDataInstall`
3. The key must be set to `<true/>`
4. The key to also include is `CriticalUpdateInstall`
5. The key must be set to `<true/>`

References:

1. https://eclecticlight.co/2021/10/27/silently-updated-security-data-files-in-monterey/
2. https://support.apple.com/en-us/HT202491
3. https://support.apple.com/guide/security/protecting-against-malware-sec469d47bd8/web
4. https://support.apple.com/guide/deployment/rapid-security-responses-dep93ff7ea78/1/web/1.0

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.7 Remediate Detected Vulnerabilities Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

1.6 Ensure Software Update Deferment Is Less Than or Equal to 30 Days (Automated)

Profile Applicability:

- Level 1

Description:

Apple provides the capability to manage software updates on Apple devices through mobile device management. Part of those capabilities permit organizations to defer software updates and allow for testing. Many organizations have specialized software and configurations that may be negatively impacted by Apple updates. If software updates are deferred, they should not be deferred for more than 30 days. This control only verifies that deferred software updates are not deferred for more than 30 days.

Note: Software deferment is deprecated by Apple and will be removed in a future OS release/update. Apple Device Management Profile - SoftwareUpdate

Rationale:

Apple software updates almost always include security updates. Attackers evaluate updates to create exploit code in order to attack unpatched systems. The longer a system remains unpatched, the greater an exploit possibility exists in which there are publicly reported vulnerabilities.

Software updates being deferred are specifically referring to OS updates and not either major upgrades (ex. upgrading from macOS 15.0 to macOS 26) or applications from the App Store.

Impact:

Some organizations may need more than 30 days to evaluate the impact of software updates.

Internal Only - General

Audit:

Perform the following to ensure that software updates are deferred at most 30 days:

Graphical Method:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that `Deferred Software Update Delays (Days)` is set to ≤ 30

Terminal Method:

Run the following command to verify that a profile is installed that defers software updates to at most 30 days:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('enforcedSoftwareUpdateDelay').js
EOS
```

If there is an output, it should be ≤ 30.

Note: If your organization does not use a software deferment mobile configuration, there will be no output and will pass the audit.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `enforcedSoftwareUpdateDelay`
3. The key must be set to `<integer><1-30></integer>`

Note: The key `enforcedSoftwareUpdateDelay` is for all updates through software updates. If your organization needs to delay major OS upgrades on a separate timescale than minor OS updates (or App Store updates), see the Additional Information section for a breakdown of what keys to use.

References:

1. https://support.apple.com/guide/deployment/about-software-updates-depc4c80847a/web

Internal Only - General

Additional Information:

The keys to enforce updates by type are as follows:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `enforcedSoftwareUpdateDelay`
3. The key must be set to `<integer><1-30></integer>`
4. The key to include is `forceDelayedSoftwareUpdates`
5. The key must be set to `<true/>`

Note: These 5 items are required to be in the configuration profile no matter what configuration you are using.

For minor update delays:

6. The key to include is `enforcedSoftwareUpdateMinorOSDeferredInstallDelay`
7. The key must be set to `<integer><1-30></integer>`

For major OS upgrade delays:

6. The key to include is `enforcedSoftwareUpdateMajorOSDeferredInstallDelay`
7. The key must be set to `<integer><set to your organization's requirements></integer>`
8. The key to include is `forceDelayedMajorSoftwareUpdates`
9. The key must be set to `<true/>`

Note: The major deferment key will still show major upgrades being unavailable unless the `PayloadScope` of the mobile configuration profile fire is set to user and not system, ie. `<string>User</string>`

For App Store update delays:

10. The key to include is `enforcedSoftwareUpdateNonOSDeferredInstallDelay`
11. The key must be set to `<integer><1-30></integer>`
12. The key to include is `forceDelayedAppSoftwareUpdates`
13. The key must be set to `<true/>`

Note: For every setting that your organization requires, it must be included in the same configuration profile. If each key is set it separate profiles it will not function.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

2 System Settings

This section contains recommendations related to configurable options in the `System Settings` application.

At Apple's World Wide Developer Conference (WWDC) 2024, Apple announced Apple Intelligence as a new feature within both macOS 15 and iOS 18. As of macOS 15.0.1, Apple has not released any of the Apple Intelligence capabilities within the operating system. Those features may be released in future versions based on Apple announcements of future releases of macOS 15.x. There is ongoing discussion within the CIS macOS community on what recommendations will be forthcoming. Those recommendations will be based on released software from Apple. Organizations need to do their own risk analysis on using Apple's first-party Apple Intelligence features. CIS will provide further guidance as the first-party functionality is released in future versions of macOS. The current consensus is around third-party integrations (i.e. ChatGPT). It is highly recommendation that these integrations are disabled until data loss prevention and confidential information controls are evaluated.

Internal Only - General

2.1 Apple Account

Apple is a hardware manufacturer that develops operating systems for the hardware it creates. Apple is also a cloud service provider, and those services include applications, music, books, television, cloud storage, etc. Apple simplifies the process to ensure that all user devices are entitled to content where the user has purchased access, or is part of an Apple basic level of entitlement (BLE) for purchasing an Apple device. The use of an Apple Account allows for a consistent access and experience across all Apple devices. An Apple Account functions as Single Sign-On access to all Apple-provided services. It is critical that each user's account is protected appropriately so that unauthorized access risk is heavily mitigated.

In rare cases, Apple will send a threat notification to a user where attempts to compromise an Apple Account have been observed. Apple will NOT send you a link to sign in to your Apple Account but will direct you to sign in through account.apple.com.

Managed Apple Accounts are a type of Apple Account managed by organizations and not owned by individual users. Not all Apple Account services are available to managed Apple Accounts. Apple keeps a list of available services here: Service access with Managed Apple Accounts

- Manage and use your Apple Account
- If you forgot your Apple Account primary email address or phone number
- To find out what devices are signed into an Apple Account, follow these instructions: Check your Apple Account device list to find where you're signed in
- To erase a macOS device and restore it to factory settings, follow these instructions: Erase your Mac and reset it to factory settings
- To learn more about Threat Notifications: About Apple threat notifications and protecting against mercenary spyware and What to do if Apple contacts you about malware or security
- Apple Account Wikipedia page
- What Is an Apple ID/Apple Account? Is it Different from iTunes and iCloud?
- Apple Account support page
- RIP Apple ID: How to Manage Your Apple Account From Anywhere

Note: Previous to WWDC 2024, Apple Accounts were called Apple IDs. There is still a large amount of media out there that will refer to Apple Accounts as Apple IDs, but the two are the same service and should not cause any confusion.

Internal Only - General

2.1.1 iCloud

iCloud is Apple's service for synchronizing, storing, and backing up data from Apple applications in both macOS and iOS.

macOS controls for iCloud are part of the Apple Account settings in macOS. The configuration options in macOS resemble the options in iOS.

Apple's iCloud is a consumer-oriented service that allows a user to store data as well as find, control, and back up devices that are associated with their Apple Account. The use of iCloud on Enterprise devices should align with the acceptable use policy for devices that are managed, as well as confidentiality requirements for data handled by the user. If iCloud is allowed, the data that is copied to Apple servers will likely be duplicated on both personal as well as Enterprise devices.

For many users, the Enterprise email system may replace many of the available features in iCloud. Calendars, notes, and contacts can sync to the official Enterprise repository and be available through multiple devices if using either an Exchange or Google environment email.

Depending on workplace requirements, it may not be appropriate to intermingle Enterprise and personal bookmarks, photos, and documents. Since the service allows every device associated with the user's Apple Account to synchronize and have access to the cloud storage, the concern is not just about having sensitive data on Apple's servers, but also having that same data on the phone of the teenage son or daughter of an employee. The use of family sharing options can reduce the risk.

Apple's iCloud is just one of many cloud-based solutions being used for data synchronization across multiple platforms, and it should be controlled consistently with other cloud services in your environment. Work with your employees and configure the access to best enable data protection for your mission.

iCloud can also sync a user's photos. If this feature is used where an organization's proprietary photos are stored, unauthorized access in a commercial cloud will result.

We are not giving any specific guidance on how your organization should configure iCloud. To verify, or modify, the iCloud settings you can refer to Apple's support documents: Change iCloud settings on Mac

Internal Only - General

2.1.1.1 Audit iCloud Passwords & Keychain (Manual)

Profile Applicability:

- Level 2

Description:

The iCloud Passwords & Keychain is Apple's synchronization service that works with Apple Accounts to synchronize password, passkey, and credit card information across macOS, iOS, iPadOS. The capability allows users to use synced password, passkey, and credit card information in either macOS, iOS, or iPadOS for use in Safari and other applications.

The password, passkey, and credit card information stored on macOS in the keychain is stored in Apple's cloud, including on Enterprise-managed computer.

When using personal Apple Accounts and credentials may include both enterprise-related and personal data, depending on user behavior and account usage patterns.

Rationale:

Ensure that iCloud Passwords and Keychain usage aligns with organizational requirements, taking into account whether personal or managed Apple Accounts are being utilized.

Impact:

When iCloud Passwords & Keychain is turned off, password, passkey, and credit card information are no longer synchronized across devices signed in with the same Apple Account. Passwords, passkeys, and credit card information can still be stored locally and accessed through the Passwords and Keychain apps, even when iCloud Passwords & Keychain is turned off.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify a profile is installed for the iCloud Passwords & Keychain sync service:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Disallow iCloud Keychain Sync` set to your organization's requirements

Terminal Method:

Run the following command to verify that a profile is installed that sets iCloud Passwords & Keychain sync to your organization's settings:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudKeychainSync').js
EOS
```

If the output is `false`, iCloud Passwords & Keychain Sync is disabled. If the output is `true`, iCloud Passwords & Keychain sync is enabled.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowCloudKeychainSync`
3. The key should be set `<true/>`, to allow iCloud Passwords & Keychain syncing, or `<false/>`, to disable it, based on your organization's requirements

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.1.1.2 Audit iCloud Drive (Manual)

Profile Applicability:

- Level 2

Description:

iCloud Drive is Apple's storage solution for applications on both macOS and iOS to use the same files that are resident in Apple's cloud storage. The iCloud Drive folder is available much like Dropbox, Microsoft OneDrive, or Google Drive.

One of the concerns in public cloud storage is that proprietary data may be inappropriately stored in an end user's personal repository. Organizations that need specific controls on information should ensure that this service is turned off or the user knows what information must be stored on services that are approved for storage of controlled information.

Rationale:

Organizations should review third party storage solutions pertaining to existing data confidentiality and integrity requirements.

Impact:

Users will not be able to use continuity on macOS to resume the use of newly composed but unsaved files.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify if a profile is installed to configure iCloud Drive:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Disallow iCloud Drive` set to your organization's requirements

Terminal Method:

Run the following command to verify that a profile is installed that sets iCloud Drive sync to your organization's settings:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudDocumentSync').js
EOS
```

If the output is `false`, iCloud Drive Sync is disabled. If the output is `true`, iCloud Drive sync is enabled.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowCloudDocumentSync`
3. The key should be set `<true/>`, to allow iCloud Drive, or `<false/>`, to disable it, based on your organization's requirements

References:

1. https://developer.apple.com/documentation/devicemanagement/restrictions

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.1.1.3 Ensure iCloud Drive Document and Desktop Sync Is Disabled (Automated)

Profile Applicability:

- Level 2

Description:

With macOS 10.12, Apple introduced the capability to have a user's Desktop and Documents folders automatically synchronize to the user's iCloud Drive, provided they have enough room purchased through Apple on their iCloud Drive. This capability mirrors what Microsoft is doing with the use of OneDrive and Office 365. There are concerns with using this capability.

The storage space that Apple provides for free is used by users with iCloud mail, all of a user's Photo Library created with the ever larger Multi-Pixel iPhone cameras, and all iOS Backups. Adding a synchronization capability for users who have files going back a decade or more, storage may be tight using the free 5GB provided without purchasing much larger storage capacity from Apple. Users with multiple computers running 10.12 and above with unique content on each will have issues as well.

Enterprise users may not be allowed to store Enterprise information in a third-party public cloud. In previous implementations, such as iCloud Drive or DropBox, the user selected what files were synchronized even if there were no other controls. The new feature synchronizes all files in a folder widely used to put working files.

The automatic synchronization of all files in a user's Desktop and Documents folders should be disabled.

https://derflounder.wordpress.com/2016/09/23/icloud-desktop-and-documents-in-macos-sierra-the-good-the-bad-and-the-ugly/

Rationale:

Automated Document synchronization should be planned and controlled to approved storage.

Impact:

Users will not be able to use iCloud for the automatic sync of the Desktop and Documents folders.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify if Desktop and Documents in iCloud Drive is enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Disallow iCloud Desktop & Documents Sync` set to `True`

Terminal Method:

Run the following command to verify that a profile is installed that disables iCloud Document and Desktop Sync:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudDesktopAndDocuments').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowCloudDesktopAndDocuments`
3. The key must be set to `<false/>`

References:

1. https://developer.apple.com/documentation/devicemanagement/restrictions

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.1.1.4 Audit Security Keys Used With Apple Accounts (Manual)

Profile Applicability:

- Level 2

Description:

Apple has introduced the capability of using security keys to protect Apple Accounts using two-factor authentication in macOS 13.2, in iOS 16.3, and in iPadOS 16.3. This feature along with the purchase of two hardware tokens (a backup device is required) protects against the compromise of Apple Accounts. This feature requires all devices using an enrolled Apple Account to meet the minimum OS standard.

Rationale:

Users of Apple devices are supported across their devices by using the same Apple Account to support shared data in both iCloud and across devices. Compromising an Apple Account has become a very attractive target for attackers to gain unauthorized access to iCloud storage and user devices. Two-factor authentication reduces the risk.

Impact:

Legacy devices and test machines will be challenging to ensure that they are all running recent Operating Systems that can utilize Security Keys. It is best practice not to use Apple Accounts with access to current user data on legacy and test machines. Technical staff that use legacy devices are encouraged to create additional Apple Accounts that do not need two-factor protection and can be used for testing on legacy devices when required.

Audit:

Graphical Method:

Perform the following steps to verify if Security Keys is set to your organization's requirements:

1. Open `System Settings`
2. Select `Apple Account`
3. Select `Password & Security`
4. Verify that `Security Keys` is set to your organization's requirements

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to set Security Keys is set to your organization's requirements:

1. Open `System Settings`
2. Select `Apple Account`
3. Select `Password & Security`
4. Select `Add..` to add a security key, or `Remove All Security Keys` ro remove security keys, to meet your organization's requirements

References:

1. https://support.apple.com/en-us/102637
2. https://9to5mac.com/2023/02/03/ios-16-3-hardware-security-keys-explained-video/
3. https://hcsonline.com/images/PDFs/Security_Key_Apple_ID.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

2.1.1.5 Audit Freeform Sync to iCloud (Manual)

Profile Applicability:

- Level 2

Description:

Starting with macOS 13.1 Apple has made FreeForm, a collaboration tool, available for macOS, iOS and iPadOS. This application allows for extensive whiteboard creation and sharing using iCloud. Organizations may want to audit the use of Freeform iCloud sharing of internally created boards.

Rationale:

Internally created whiteboards may not be authorized to share to external contacts through iCloud.

Audit:

Graphical Method:

Perform the following steps to verify if iCloud Freeform sync is enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Disallow iCloud Freeform Sync` set to your organization's requirement

Terminal Method:

Run the following command to verify that a profile is installed that disables Freeform Sync:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudFreeform').js
EOS
```

The output should match your organization's requirement

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowCloudFreeform`
3. The key must be set to `<<true/false>/>`

Internal Only - General

References:

1. https://www.apple.com/newsroom/2022/12/apple-launches-freeform-a-powerful-new-app-designed-for-creative-collaboration/
2. https://support.apple.com/guide/freeform/share-a-board-frfma5307056b/mac
3. https://support.apple.com/guide/icloud/set-up-freeform-mmd1b86048ac/icloud

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.1.1.6 Audit Find My Mac (Manual)

Profile Applicability:

- Level 2

Description:

Find My is Apple's consumer solution for device tracking of your devices. This allows a user to track the location of devices associated with their Apple Account. This is a great solution for consumer or user device management and tracking, but it is not meant to be an enterprise management solution to device tracking and information management on enterprise managed devices. There are multiple enterprise MDM solutions for managing organizational devices.

Rationale:

An enterprise solution should be used for tracking and information management of all devices, including Apple devices. Apple's Find My solution only handles Apple devices. If no enterprise solution is available, Find My provides capabilities for a user to manage and track Apple devices. It is not designed as an enterprise solution, and should not be used as one. It is better to allow the user to track devices that use their Apple Account than to have no tracking at all.

Impact:

There should be no impact on the user while using the device. If someone other than the user has access to tracking information, this can impact the user and needs to be researched. Users should audit to ensure that only authorized people have access to your location. Using multiple solutions for device tracking can unnecessary complexity.

One of the advantages of Find My... is that personal tracking is under the context of the user that is signed into their Apple Account on devices and that is secured against unauthorized access. Blocking this solution in favor of enterprise tools could result in personal information loss including the collection, and possible misuse, of personal location information. Organizations should make a risk assessment on device/user tracking for internal use only.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify if Security Keys is set to your organization's requirements:

1. Open `System Settings`
2. Select `Apple Account`
3. Select `iCloud`
4. Select `Show More Apps..`
5. Verify that `Find My Mac` is set to your organization's requirements

Terminal Method:

Run the following command to verify that a profile is installed that disables iCloud Document and Desktop Sync:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowFindMyDevice').js
EOS
```

The output will either be `true`, Find My Device is enabled, or `false`, Find My Device is disabled depending on your organizations requirements.

Remediation:

Graphical Method:

Perform the following steps to set Security Keys is set to your organization's requirements:

1. Open `System Settings`
2. Select `Apple Account`
3. Select `iCloud`
4. Select `Show More Apps..`
5. Set `Find My Mac` is set to your organization's requirements

Internal Only - General

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowFindMyDevice`
3. The key must be set to `<<true/>or<false/>>` depending on your organization's requirements

Note: Find My Device should only be disabled if your organization is using an enterprise solution for tracking devices.

Note: This key does not fully disable Find My Device. It removes the Device tab in the Find My... app. The key `allowFindMyFriends` can also be used to disable the Friends tab in the app as well. The `DisableFMMiCloudSetting` key in the `com.apple.icloud.managed` PaylodType can disable the Find My setting, but does not disable it if it is already enabled.

References:

1. https://www.icloud.com/find/
2. https://support.apple.com/lt-lt/guide/deployment/depdc4ba8d82/web
3. https://www.apple.com/legal/privacy/data/en/find-my
4. https://support.apple.com/lt-lt/guide/apple-business-manager/axm812df1dd8/1/web

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.1.2 Audit App Store Password Settings (Manual)

Profile Applicability:

- Level 2

Description:

With Mac OS X 10.11, Apple added settings for password storage for the App Store in macOS. These settings parallel the settings in iOS. As with iOS, the choices are a requirement to provide a password after every purchase or to have a 15-minute grace period, and whether or not to require a password for free purchases. The response to this setting is stored in a cookie and processed by iCloud.

There is plenty of risk information on the wisdom of this setting for parents with children buying games on iPhones and iPads. The most relevant information here is the likelihood that users who are not authorized to download software may have physical access to an unlocked computer where someone who is authorized recently made a purchase. If that is a concern, a password should be required at all times for App Store access in the Password Settings controls.

Rationale:

Audit:

Graphical Method:

Perform the following steps to verify that App Store Passwords are set to your organization's requirements:

1. Open `System Settings`
2. Select `Apple Account`
3. Select `Media & Purchases`
4. Verify that `Free Downloads` is set to your organization's requirements
5. Verify that `Purchases and In-App Purchases` is set to your organization's requirements

Remediation:

Graphical Method:

Perform the following steps to set App Store Passwords to your organization's requirements:

1. Open `System Settings`
2. Select `Apple Account`
3. Select `Media & Purchases`
4. Set `Free Downloads` to your organization's requirements
5. Set `Purchases and In-App Purchases` to your organization's requirements

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.2 Network

The `Network System Settings` pane includes the firewall settings. macOS has a built-in firewall that has two main configuration aspects. Both the Application Layer Firewall (ALF) and the Packet Filter Firewall (PF) can be used to secure running ports and services on a Mac. The Application Firewall is the one accessible in System Preferences under Security. The PF firewall contains many more capabilities than ALF, but also requires a greater understanding of firewall recipes and rule configurations. For standard use cases on a Mac, the PF firewall is not necessary. macOS may expose server services that are reachable remotely, but that is not the primary use case or design. If custom use cases are required, the PF firewall can provide additional security. Macs that are used as mobile desktops do not need to use the PF firewall capabilities unless permanently open ports need to be protected with more granular IP access controls.

Additional information

https://www.muo.com/tag/mac-really-need-firewall/

https://blog.neilsabol.site/post/quickly-easily-adding-pf-packet-filter-firewall-rules-macos-osx/

http://marckerr.com/a-simple-guild-to-the-mac-pf-firewall/

https://blog.scottlowe.org/2013/05/15/using-pf-on-os-x-mountain-lion/

Internal Only - General

2.2.1 Ensure Firewall Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

A firewall is a piece of software that blocks unwanted incoming connections to a system. The socketfilter Firewall is what is used when the Firewall is turned on in the Security & Privacy Preference Pane. Logging is required to appropriately monitor what access is allowed and denied. The logs can be viewed in the macOS Unified Logs.

Pprior to macOS 15.0 Sequoia, there were additional step to turn on firewall logging after enabling the firewall. As of macOS 15, logging is turned on automatically without user interaction. The logging recommendation has been removed in the macOS 15 benchmark and will not be included going forward. If your organization is looking for more detailed information about network security, you will need a third-party solution.

Rationale:

A firewall minimizes the threat of unauthorized users gaining access to your system while connected to a network or the Internet.

Impact:

The firewall may block legitimate traffic. Applications that are unsigned will require special handling.

Audit:

Graphical Method:

Perform the following steps to ensure the firewall is enabled:

1. Open `System Settings`
2. Select `Network`
3. Verify that the `Firewall` is `Active`

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Firewall` set to `Enabled`

Internal Only - General

Terminal Method:

Run the following command to verify that the firewall is enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableFirewall').js
EOS

true
```

Also, the status of the firewall can be checked with the binary. Run the following command to verify if the firewall is enabled with the binary:

```
% /usr/bin/sudo /usr/libexec/ApplicationFirewall/socketfilterfw --
getglobalstate
```

The output will either be `Firewall is enabled. (State = 1)` or `Firewall is enabled. (State = 2)` if the firewall is enabled. If the firewall is disabled, the output will be `Firewall is disabled. (State = 0)`

Remediation:

Graphical Method:

Perform the following steps to turn the firewall on:

1. Open `System Settings`
2. Select `Network`
3. Select `Firewall`
4. Set `Firewall` to enabled

Terminal Method:

Run the following command to enable the firewall:

```
% /usr/bin/sudo /usr/libexec/ApplicationFirewall/socketfilterfw  --
setglobalstate on
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.security.firewall`
2. The key to include is `EnableFirewall`
3. The key must be set to `<true/>`

References:

1. https://support.apple.com/guide/security/firewall-security-in-macos-seca0e83763f/web
2. https://support.apple.com/guide/mac-help/block-connections-to-your-mac-with-a-firewall-mh34041/mac

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.1 Centralize Security Event Alerting Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.5 Implement Application Firewalls Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			●

Internal Only - General

2.2.2 Ensure Firewall Stealth Mode Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

While in Stealth mode, the computer will not respond to unsolicited probes, dropping that traffic.

Rationale:

Stealth mode on the firewall minimizes the threat of system discovery tools while connected to a network or the Internet.

Impact:

Traditional network discovery tools like ping will not succeed. Other network tools that measure activity and approved applications will work as expected.

This control aligns with the primary macOS use case of a laptop that is often connected to untrusted networks where host segregation may be non-existent. In that use case, hiding from the other inmates is likely more than desirable. In use cases where use is only on trusted LANs with static IP addresses, stealth mode may not be desirable.

Audit:

Graphical Method:

Perform the following steps to verify the firewall has stealth mode enabled:

1. Open `System Settings`
2. Select `Network`
3. Select `Firewall`
4. Select `Option`
5. Verify that `Enable stealth mode` is enabled

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Stealth Mode` set to `Enabled`

Internal Only - General

Terminal Method:

Run the following command to verify that stealth mode is enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableStealthMode').js
EOS

true
```

Also, the status of the stealth mode can be checked with the binary. Run the following command to verify if the firewall is enabled with the binary:

```
% /usr/libexec/ApplicationFirewall/socketfilterfw --getstealthmode

Firewall stealth mode is on
```

Remediation:

Graphical Method:

Perform the following steps to enable firewall stealth mode:

1. Open `System Settings`
2. Select `Network`
3. Select `Firewall`
4. Select `Options...`
5. Set `Enabled stealth mode` to enabled

Terminal Method:

Run the following command to enable stealth mode:

```
% /usr/bin/sudo /usr/libexec/ApplicationFirewall/socketfilterfw --
setstealthmode on

Stealth mode enabled
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.security.firewall`
2. The key to include is `EnableStealthMode`
3. The key must be set to `<true/>`

Note: This key must be set in the same configuration profile with `EnableFirewall` set to `<true/>`. If it is set in its own configuration profile, it will fail.

References:

1. http://support.apple.com/en-us/HT201642

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

Internal Only - General

2.3 General

Internal Only - General

2.3.1 AirDrop & Handoff

Internal Only - General

2.3.1.1 Ensure AirDrop Is Disabled When Not Actively Transferring Files (Automated)

Profile Applicability:

- Level 1

Description:

AirDrop is Apple's built-in, on-demand, ad hoc file exchange system that is compatible with both macOS and iOS. It uses Bluetooth LE for discovery that limits connectivity to Mac or iOS users that are in close proximity. Depending on the setting, it allows everyone or only Contacts to share files when they are near each other.

In many ways, this technology is far superior to the alternatives. The file transfer is done over a TLS encrypted session, does not require any open ports that are required for file sharing, does not leave file copies on email servers or within cloud storage, and allows for the service to be mitigated so that only people already trusted and added to contacts can interact with you.

While there are positives to AirDrop, there are privacy concerns that could expose personal information. For that reason, AirDrop should be disabled, and should only be enabled when needed and disabled afterwards. The recommendation against enabling the sharing is not based on any known lack of security in the protocol, but for specific user operational concerns.

- If AirDrop is enabled, the Mac is advertising that a Mac is addressable on the local network and open to either unwanted AirDrop upload requests or for a negotiation on whether the remote user is in the user's contacts list. Neither process is desirable.
- In most known use cases, AirDrop use qualifies as ad hoc networking when it involves Apple device users deciding to exchange a file using the service. AirDrop can thus be enabled on the fly for that exchange.

For organizations concerned about any use of AirDrop because of Digital Loss Prevention (DLP) monitoring on other protocols, Jamf has an article on reviewing AirDrop logs.

Detecting outbound AirDrop transfers and logging them

Rationale:

AirDrop can allow malicious files to be downloaded from unknown sources. Contacts Only limits may expose personal information to devices in the same area.

Impact:

Disabling AirDrop can limit the ability to move files quickly over the network without using file shares.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure that AirDrop is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow AirDrop` set to `False`

Terminal Method:

Run the following command to verify that a profile is installed that disabled AirDrop:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAirDrop').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowAirDrop`
3. The key must be set to `<false/>`

Note: AirDrop can only be enabled or disabled through configuration profiles. If your organization wants to use AirDrop, it would need to be set through Terminal or the GUI.

References:

1. https://www.techrepublic.com/article/apple-airdrop-users-reportedly-vulnerable-to-security-flaw/
2. https://www.imore.com/how-apple-keeps-your-airdrop-files-private-and-secure
3. https://en.wikipedia.org/wiki/AirDrop
4. https://macmost.com/10-reasons-you-should-be-using-airdrop-to-transfer-files.html

Additional Information:

To configure AirDrop with more granularity than the profile allows, your organization should look into third-party applications. An example is Air Drop Assistant.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	15.4 Disable Wireless Access on Devices if Not Required Disable wireless access on devices that do not have a business purpose for wireless access.			●

Internal Only - General

2.3.1.2 Ensure AirPlay Receiver Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

In macOS Monterey (12.0), Apple has added the capability to share content from another Apple device to the screen of a host Mac. While there are many valuable uses of this capability, such sharing on a standard Mac user workstation should be enabled ad hoc as required rather than allowing a continuous sharing service. The feature can be restricted by Apple Account or network and is configured to use by accepting the connection on the Mac. Part of the concern is frequent connection requests may function as a denial-of-service and access control limits may provide too much information to an attacker.

https://macmost.com/how-to-use-a-mac-as-an-airplay-receiver.html

https://support.apple.com/guide/mac-pro-rack/use-airplay-apdf1417128d/mac

Rationale:

This capability appears very useful for kiosk and shared work spaces. The ability to allow by network could be especially useful on segregated guest networks where visitors could share their screens on computers with bigger monitors, including computers connected to projectors.

Impact:

Turning off AirPlay sharing by default will not allow users to share without turning the service on. The service should be enabled as needed rather than left on.

Audit:

Graphical Method:

Perform the following steps to ensure that AirPlay Receiver is Disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow AirPlay Incoming Requests` set to `False`

Internal Only - General

Terminal Method:

For each user, run the following command to verify that AirPlay Receiver is disabled:

Run the following command to verify that a profile is installed that disables the ability to use the computer as an AirPlay Receiver:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAirPlayIncomingRequests').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowAirPlayIncomingRequests`
3. The key must be set to `<false/>`

Default Value:

AirPlay Receiver is enabled by default.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.2 Date & Time

This section contains recommendations related to the configurable items under the `Date & Time` panel.

Internal Only - General

2.3.2.1 Ensure Set Time and Date Automatically Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Correct date and time settings are required for authentication protocols, file creation, modification dates, and log entries.

Note: If your organization has internal time servers, enter them here. Enterprise mobile devices may need to use a mix of internal and external time servers. If multiple servers are required, use the Date & Time System Preference with each server separated by a space.

Additional Note: The default Apple time server is time.apple.com. Variations include time.euro.apple.com. While it is certainly more efficient to use internal time servers, there is no reason to block access to global Apple time servers or to add a time.apple.com alias to internal DNS records. There are no reports that Apple gathers any information from NTP synchronization, as the computers already phone home to Apple for Apple services including iCloud use and software updates. Best practice is to allow DNS resolution to an authoritative time service for time.apple.com, preferably to connect to Apple servers, but local servers are acceptable as well.

Rationale:

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features.

Impact:

The `timed` service will periodically synchronize with named time servers and will make the computer time more accurate.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure that the system's date and time are set automatically:

1. Open `System Settings`
2. Select `General`
3. Select `Date & Time`
4. Verify that `Set time and date automatically` is enabled

Terminal Method:

Run the following command to ensure that date and time are automatically set:

```
% /usr/bin/sudo /usr/sbin/systemsetup -getusingnetworktime

Network Time: On
```

Remediation:

Graphical Method:

Perform the following to enable the date and time to be set automatically:

1. Open `System Settings`
2. Select `General`
3. Select `Date & Time`
4. Set `Set time and date automatically` to enabled

Note: By default, the operating system will use `time.apple.com` as the time server. You can change to any time server that meets your organization's requirements.

Internal Only - General

Terminal Method:

Run the following commands to enable the date and time setting automatically:

```
% /usr/bin/sudo /usr/sbin/systemsetup -setnetworktimeserver
<your.time.server>

setNetworkTimeServer: <your.time.server>

% /usr/bin/sudo /usr/sbin/systemsetup -setusingnetworktime on

setUsingNetworkTime: On
```

example:

```
% /usr/bin/sudo /usr/sbin/systemsetup -setnetworktimeserver time.apple.com

setNetworkTimeServer: time.apple.com

% /usr/bin/sudo /usr/sbin/systemsetup -setusingnetworktime on

setUsingNetworkTime: On
```

Run the following commands if you have not set, or need to set, a new time zone:

```
% /usr/bin/sudo /usr/sbin/systemsetup -listtimezones

% /usr/bin/sudo /usr/sbin/systemsetup -settimezone <selected time zone>
```

example:

```
% /usr/bin/sudo /usr/sbin/systemsetup -listtimezones

Time Zones:
 Africa/Abidjan
 Africa/Accra
 Africa/Addis_Ababa
 ...


$ /usr/bin/sudo /usr/sbin/systemsetup -settimezone America/New_York

Set TimeZone: America/New_York
```


Internal Only - General

Additional Information:

To learn more about `timed`, read: Has anyone got the time? How High Sierra has changed time synchronisation

Also, Ensure that time on the computer is within acceptable limits. Truly accurate time is measured within milliseconds.

Run the following commands to verify the time is set within an appropriate limit:

```
% /usr/bin/sudo /usr/sbin/systemsetup -getnetworktimeserver
```

The output will include `Network Time Server:` and the name of your time server.

example: `Network Time Server: time.apple.com`

```
% /usr/bin/sudo /usr/bin/sntp <your.time.server>
```

Ensure that the offset result(s) are between -270.x and 270.x seconds.

And to set the time to the correct offset:

```
% /usr/bin/sudo /usr/bin/sntp -sS <your.time.server>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

Internal Only - General

2.3.2.2 Ensure the Time Service Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

In macOS 10.14, Apple replace `ntp` with `timed` for time services, and is used to ensure correct time is kept. Correct date and time settings are required for authentication protocols, file creation, modification dates and log entries.

Rationale:

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features.

Impact:

Accurate time is required for many computer functions.

Audit:

Terminal Method:

Run the following command to ensure that the timed service is enabled:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -c com.apple.timed

1
```

Remediation:

If the `timed` service has been disabled, assume that the operating system has been compromised. Back up any files, and do a clean install to a known good Operating System.

Internal Only - General

Additional Information:

It is also recommended that time on the computer is within acceptable limits. Truly accurate time is measured within milliseconds.

Run the following commands to verify the time is set within an appropriate limit:

```
% /usr/bin/sudo /usr/sbin/systemsetup -getnetworktimeserver
```

The output will include `Network Time Server:` and the name of your time server.

example: `Network Time Server: time.apple.com`

```
% /usr/bin/sudo /usr/bin/sntp <your.time.server>
```

Ensure that the offset result(s) are between -270.x and 270.x seconds.

And to set the time to the correct offset:

```
% /usr/bin/sudo /usr/bin/sntp -sS <your.time.server>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

Internal Only - General

2.3.3 Sharing

This section contains recommendations related to the configurable items under the `Sharing` panel.

With the release of macOS 14.0 Sonoma, Apple has added configuration profile options in the payloadtype `com.apple.applicationaccess` for the following sharing settings:

- Remote Management `allowARDRemoteManagementModification`
- Bluetooth Sharing `allowBluetoothSharingModification`
- File Sharing `allowFileSharingModification`
- Internet Sharing `allowInternetSharingModification`
- Printer Sharing `allowPrinterSharingModification`
- Remote Apple Events `allowRemoteAppleEventsModification`

These keys will disable the ability to modify sharing settings in the GUI only. They do not modify or disable modification through the binary or disable the service. These keys are not being included in the benchmark beyond this note for that reason, as well as the fact that they can make an administrator's job more difficult to properly access and remediate the security posture of the system.

Internal Only - General

2.3.3.1 Ensure Screen Sharing Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Screen Sharing allows a computer to connect to another computer on a network and display the computer's screen. While sharing the computer's screen, the user can control what happens on that computer, such as opening documents or applications, opening, moving, or closing windows, and even shutting down the computer.

While mature administration and management does not use graphical connections for standard maintenance, most help desks have capabilities to assist users in performing their work when they have technical issues and need support. Help desks use graphical remote tools to understand what the user sees and assist them so they can get back to work. For macOS, some of these remote capabilities can use Apple's OS tools. Control is therefore not meant to prohibit the use of a just-in-time graphical view from authorized personnel with authentication controls. Sharing should not be enabled except in narrow windows when help desk support is required.

Screen Sharing on macOS can allow the use of the insecure VNC protocol. VNC is a clear text protocol that should not be used on macOS.

Rationale:

Disabling Screen Sharing mitigates the risk of remote connections being made without the user of the console knowing that they are sharing the computer.

Impact:

Help desks may require the periodic use of a graphical connection mechanism to assist users. Any support that relies on native macOS components will not work unless a scripted solution to enable and disable sharing is used, as necessary.

Audit:

Graphical Method:

Perform the following steps to ensure Screen Sharing is not enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Screen Sharing` is not enabled

Internal Only - General

Terminal Method:

Run the following commands to verify that Screen Sharing is not set:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -E
"com.apple.screensharing$"
```

There will be no output if the service is disabled. If there is an output, then that is a finding.

Remediation:

Graphical Method:

Perform the following steps to disable Screen Sharing:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `Screen Sharing` to disabled

Terminal Method:

Run the following command to turn off Screen Sharing:

```
% /usr/bin/sudo /bin/launchctl disable system/com.apple.screensharing

% /usr/bin/sudo /bin/launchctl bootout system/com.apple.screensharing
```

References:

1. https://support.apple.com/guide/mac-help/turn-screen-sharing-on-or-off-mh11848/mac

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.2 Ensure File Sharing Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

File sharing from a user workstation creates additional risks, such as:

- Open ports are created that can be probed and attacked
- Passwords are attached to user accounts for access that may be exposed and endanger other parts of the organizational environment, including directory accounts
- Increased complexity makes security more difficult and may expose additional attack vectors

Apple's File Sharing uses the Server Message Block (SMB) protocol to share to other computers that can mount SMB shares. This includes other macOS computers.

Apple warns that SMB sharing stored passwords is less secure, and anyone with system access can gain access to the password for that account. When sharing with SMB, each user accessing the Mac must have SMB enabled. Storing passwords, especially copies of valid directory passwords, decreases security for the directory account and should not be used.

Rationale:

By disabling File Sharing, the remote attack surface and risk of unauthorized access to files stored on the system is reduced.

Impact:

File Sharing can be used to share documents with other users, but hardened servers should be used rather than user endpoints. Turning on File Sharing increases the visibility and attack surface of a system unnecessarily.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure that File Sharing is not enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `File Sharing` is not enabled

Terminal Method:

Run the following command to verify that File Sharing is not enabled:

```
% /usr/bin/sudo /bin/launchctl list | grep -c "com.apple.smbd"

0
```

Remediation:

Graphical Method:

Perform the following steps to disable File Sharing:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `File Sharing` to disabled

Terminal Method:

Run the following command to disable File Sharing:

```
% /usr/bin/sudo /bin/launchctl disable system/com.apple.smbd

% /usr/bin/sudo /bin/launchctl bootout system/com.apple.smbd
```


Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.3 Ensure Printer Sharing Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

By enabling Printer Sharing, the computer is set up as a print server to accept print jobs from other computers. Dedicated print servers or direct IP printing should be used instead.

Rationale:

Disabling Printer Sharing mitigates the risk of attackers attempting to exploit the print server to gain access to the system.

Audit:

Graphical Method:

Perform the following steps to ensure that Printer Sharing is not enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Printer Sharing` is not enabled

Terminal Method:

Run the following command to verify that Printer Sharing is not enabled:

```
% /usr/bin/sudo /usr/sbin/cupsctl | grep -c "_share_printers=0"

1
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to disable Printer Sharing:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `Printer Sharing` to disabled

Terminal Method:

Run the following command to disable Printer Sharing:

```
% /usr/bin/sudo /usr/sbin/cupsctl --no-share-printers
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.4 Ensure Remote Login Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Remote Login allows an interactive terminal connection to a computer.

Rationale:

Disabling Remote Login mitigates the risk of an unauthorized person gaining access to the system via Secure Shell (SSH). While SSH is an industry standard to connect to POSIX servers, the scope of the benchmark is for Apple macOS clients, not servers.

macOS does have an IP-based firewall available (pf, ipfw has been deprecated) that is not enabled or configured. There are more details and links in the `Network` sub-section. macOS no longer has TCP Wrappers support built in and does not have strong Brute-Force password guessing mitigations, or frequent patching of OpenSSH by Apple. Since most macOS computers are mobile workstations, managing IP-based firewall rules on mobile devices can be very resource intensive. All of these factors can be parts of running a hardened SSH server.

Impact:

The SSH server built into macOS should not be enabled on a standard user computer, particularly one that changes locations and IP addresses. A standard user that runs local applications, including email, web browser, and productivity tools, should not use the same device as a server. There are Enterprise management toolsets that do utilize SSH. If they are in use, the computer should be locked down to only respond to known, trusted IP addresses and appropriate administrator service accounts.

For macOS computers that are being used for specialized functions, there are several options to harden the SSH server to protect against unauthorized access, including brute force attacks. There are some basic criteria that need to be considered:

- Do not open an SSH server to the internet without controls in place to mitigate SSH brute force attacks. This is particularly important for systems bound to Directory environments. It is great to have controls in place to protect the system, but if they trigger after the user is already locked out of their account, they are not optimal. If authorization happens after authentication, directory accounts for users that don't even use the system can be locked out.
- Do not use SSH key pairs when there is no insight to the security on the client system that will authenticate into the server with a private key. If an attacker gets access to the remote system and can find the key, they may not need a password or a key logger to access the SSH server.
- Detailed instructions on hardening an SSH server, if needed, are available in the CIS Linux Benchmarks, but it is beyond the scope of this benchmark.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure that Remote Login is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Remote Login` is not enabled

Terminal Method:

Run the following commands to verify that Remote Login is disabled:

```
% /usr/bin/sudo /usr/sbin/systemsetup -getremotelogin

Remote Login: Off

% /usr/bin/sudo /bin/launchctl print-disabled system | /usr/bin/grep -c
'"com.openssh.sshd" => disabled'

1

% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -c "com.openssh.sshd"

0
```

Note: Previously the audit was only using `systemsetup` but after testing it was discovered that the service can still be enabled through Terminal. Going forward the audit will check the `systemsetup`, if the service is disabled, and that the service is not running at the time of the audit.

Internal Only - General

Remediation:

Perform the following to disable Remote Login:

Graphical Method:

Perform the following steps to disable Remote Login:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `Remote Login` to disabled

Terminal Method:

Run the following command to disable Remote Login:

```
% /usr/bin/sudo /usr/sbin/systemsetup -setremotelogin off

Do you really want to turn remote login off? If you do, you will lose this
connection and can only turn it back on locally at the server (yes/no)?
```

Entering yes will disable remote login.

Note: This command will disable the service as well as stop it running in time.

Additional Information:

`man sshd_config`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.5 Ensure Remote Management Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Remote Management is the client portion of Apple Remote Desktop (ARD). Remote Management can be used by remote administrators to view the current screen, install software, report on, and generally manage client Macs.

The screen sharing options in Remote Management are identical to those in the Screen Sharing section. In fact, only one of the two can be configured. If Remote Management is used, refer to the Screen Sharing section above on issues regarding screen sharing.

Remote Management should only be enabled when a Directory is in place to manage the accounts with access. Computers will be available on port 5900 on a macOS System and could accept connections from untrusted hosts depending on the configuration, which is a major concern for mobile systems. As with other sharing options, an open port even for authorized management functions can be attacked, and both unauthorized access and Denial-of-Service vulnerabilities could be exploited. If remote management is required, the pf firewall should restrict access only to known, trusted management consoles. Remote management should not be used across the Internet without the use of a VPN tunnel.

Rationale:

Remote Management should only be enabled on trusted networks with strong user controls present in a Directory system. Mobile devices without strict controls are vulnerable to exploitation and monitoring.

Impact:

Many organizations utilize ARD for client management.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify that Remote Management is not enabled:

1. Open System Settings
2. Select General
3. Select Sharing
4. Verify that Remote Management is not enabled

Terminal Method:

Run the following command to verify that Remote Management is not enabled:

```
% /usr/bin/sudo /bin/ps -ef | /usr/bin/grep -e ARDAgent

0  9233  8630   0  3:32pm ttys001    0:00.00 grep -e ARDAgent
```

Remediation:

Graphical Method:

Perform the following steps to disable Remote Management:

1. Open System Settings
2. Select General
3. Select Sharing
4. Set Remote Management to disabled

Terminal Method:

Run the following command to disable Remote Management:

```
% /usr/bin/sudo
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources
/kickstart -deactivate -stop

Starting...
Removed preference to start ARD after reboot.
Done.
```

Additional Information:

/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -help

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

Internal Only - General

2.3.3.6 Ensure Remote Apple Events Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple Events is a technology that allows one program to communicate with other programs. Remote Apple Events allows a program on one computer to communicate with a program on a different computer.

Rationale:

Disabling Remote Apple Events mitigates the risk of an unauthorized program gaining access to the system.

Impact:

With remote Apple events turned on, an AppleScript program running on another Mac can interact with the local computer.

Audit:

Graphical Method:

Perform the following steps to ensure that Remote Apple Events is not enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Remote Apple Events` is not enabled

Terminal Method:

Run the following commands to verify that Remote Apple Events is not set

```
% /usr/bin/sudo /usr/sbin/systemsetup -getremoteappleevents

Remote Apple Events: Off
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to disable Remote Apple Events:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `Remote Apple Events` to disabled

Terminal Method:

Run the following commands to set Remote Apple Events to Off:

```
% /usr/bin/sudo /usr/sbin/systemsetup -setremoteappleevents off

setremoteappleevents: Off
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.7 Ensure Internet Sharing Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Internet Sharing uses the open source `natd` process to share an internet connection with other computers and devices on a local network. This allows the Mac to function as a router and share the connection to other, possibly unauthorized, devices.

Rationale:

Disabling Internet Sharing reduces the remote attack surface of the system.

Impact:

Internet Sharing allows the computer to function as a router and other computers to use it for access. This can expose both the computer itself and the networks it is accessing to unacceptable access from unapproved devices.

Audit:

Graphical Method:

Perform the following steps to ensure Internet Sharing is not enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Internet Sharing` is not enabled

Internal Only - General

Terminal Method:

Run the following commands to verify that Internet Sharing is not set:

```
% /usr/bin/sudo /usr/bin/defaults read
/Library/Preferences/SystemConfiguration/com.apple.nat >nul 2>&1 | grep -c
"Enabled = 1;"

0
```

or

Run the following command to verify that a profile is installed that automatically disables internet sharing:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('forceInternetSharingOff').js
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to disable Internet Sharing:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `Internet Sharing` to disabled

Terminal Method:

Run the following command to turn off Internet Sharing:

```
% usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/SystemConfiguration/com.apple.nat NAT -dict Enabled -int
0
```

Note: Using the Terminal Method will not be reflected in the GUI, but will disable the underlying service.

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.MCX`
2. The key to include is `forceInternetSharingOff`
3. The key must be set to `<true/>`

Internal Only - General

References:

1. STIGID AOSX-12-001270

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.8 Ensure Content Caching Is Disabled (Automated)

Profile Applicability:

- Level 2

Description:

Starting with macOS 10.13, Apple introduced a service to make it easier to deploy data from Apple, including software updates, where there are bandwidth constraints to the Internet and fewer constraints or greater bandwidth exist on the local subnet. This capability can be very valuable for organizations that have throttled and possibly metered Internet connections. In heterogeneous enterprise networks with multiple subnets, the effectiveness of this capability would be determined by how many Macs were on each subnet at the time new, large updates were made available upstream. This capability requires the use of mac OS clients as P2P nodes for updated Apple content. Unless there is a business requirement to manage operational Internet connectivity and bandwidth, user endpoints should not store content and act as a cluster to provision data.

Content types supported by Content Caching in macOS

Rationale:

The main use case for Mac computers is as mobile user endpoints. P2P sharing services should not be enabled on laptops that are using untrusted networks. Content Caching can allow a computer to be a server for local nodes on an untrusted network. While there are certainly logical controls that could be used to mitigate risk, they add to the management complexity. Since the value of the service is in specific use cases, organizations with the use case described above can accept risk as necessary.

Impact:

This setting will adversely affect bandwidth usage between local subnets and the Internet.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure that Content Caching is not enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Content Caching` is not enabled

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow Content Caching` set to `False`

Terminal Method:

Run the following command to verify that Content Caching is not enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.AssetCache')\
  .objectForKey('Activated'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationac
cess')\
  .objectForKey('allowContentCaching'))
  if ( ( pref1 == 0 ) || ( pref2 == 0 ) ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to disable Content Caching:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `Content Caching` to disabled

Internal Only - General

Terminal Method:

Run the following command to disable Content Caching:

```
% /usr/bin/sudo /usr/bin/AssetCacheManagerUtil deactivate
```

The output will include `Content caching deactivated`

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowContentCaching`
3. The key must be set to `<false/>`

References:

1. https://support.apple.com/guide/mac-help/about-content-caching-mchl9388ba1b/
2. https://support.apple.com/guide/mac-help/set-up-content-caching-on-mac-mchl3b6c3720/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.9 Ensure Media Sharing Is Disabled (Automated)

Profile Applicability:

- Level 2

Description:

Starting with macOS 10.15, Apple has provided a control which permits a user to share Apple downloaded content on all Apple devices that are signed in with the same Apple Account. This allows users to share downloaded Movies, Music, or TV shows with other controlled macOS, iOS and iPadOS devices, as well as photos with Apple TVs.

With this capability, guest users can also use media downloaded on the computer.

The recommended best practice is not to use the computer as a server, but to utilize Apple's cloud storage in order to download and use content stored there if content stored with Apple is used on multiple devices.

https://support.apple.com/guide/mac-help/set-up-media-sharing-on-mac-mchlp13371337/mac

Note: In macOS 15.0 Sequoia, Apple added a supported profile key for Media Sharing that replaces the keys in the benchmarks in previous versions.

Rationale:

Disabling Media Sharing reduces the remote attack surface of the system.

Impact:

Media Sharing allows for pre-downloaded content on a Mac to be available to other Apple devices on the same network. Leaving this disabled forces device users to stream or download content from each Apple authorized device. This sharing could even allow unauthorized devices on the same network media access.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify that a profile is installed that disables Media Sharing:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationac
cess')\
  .objectForKey('allowMediaSharing'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationac
cess')\
  .objectForKey('allowMediaSharingModification'))
  if ( pref1 == 0 && pref2 == 0 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Note: Since the profile method sets a system-wide setting, the individual user audit and/or remediation has been removed. To be compliant, a profile must be installed for this recommendation. We have included the individual user information in the additional information section for reference only.

Note: If a user has media sharing enabled when installing the profile it will not disable media sharing, but will instead lock it as enabled. To verify that no users have media sharing enabled before installing the profile, run the following command for each user on the system:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults read
com.apple.amp.mediasharingd home-sharing-enabled
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowMediaSharing`
3. The key must be set to `<false/>`
4. The key to also include is `allowMediaSharingModification`
5. The key must be set to `<false/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.3.3.10 Ensure Bluetooth Sharing Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Bluetooth Sharing allows files to be exchanged with Bluetooth-enabled devices. This setting only disables the receiving of files and requires both devices to be paired through Bluetooth as well as accepted by the receiver. This setting does not disable the ability to send files from the device to another paired Bluetooth device.

Bluetooth pairing only requires an acceptance dialog on either device attempting to pair. It does require the Bluetooth pane in `System Settings` to be open for any macOS device to be discoverable. While it does give a verification code, it does not require either device to enter the code, but just accept the dialog box (on either device). At that point, the two devices are paired and files can be shared through Bluetooth. To receive files through `Bluetooth File Exchange` application, the user does have to accept the file(s) through a dialog box.

Users should only pair to known trusted Bluetooth devices.

Rationale:

Disabling Bluetooth Sharing minimizes the risk of an attacker using Bluetooth to remotely attack the system.

Impact:

There is a general expectation that Bluetooth peripherals will be used by most users in Apple's ecosystem. Disabling sharing should have no impact on the use of Bluetooth peripherals.

Audit:

Graphical Method:

Perform the following steps to verify that Bluetooth Sharing is not enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Bluetooth Sharing` is not enabled

Internal Only - General

Terminal Method:

Run the following command to verify that Bluetooth Sharing is disabled:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults -currentHost read
com.apple.Bluetooth PrefKeyServicesEnabled

0
% /usr/bin/sudo -u firstuser /usr/bin/defaults -currentHost read
com.apple.Bluetooth PrefKeyServicesEnabled

0
```

Remediation:

Graphical Method:

Perform the following steps to disable Bluetooth Sharing:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Set `Bluetooth Sharing` to disabled

Terminal Method:

Run the following command to disable Bluetooth Sharing is disabled:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults -currentHost write
com.apple.Bluetooth PrefKeyServicesEnabled -bool false
% /usr/bin/sudo -u firstuser /usr/bin/defaults -currentHost write
com.apple.Bluetooth PrefKeyServicesEnabled -bool false
```

Additional Information:

Since we are not giving DLP based recommendations, this recommendation has been moved to a manual setting. For more stringent control of Bluetooth, your organization should use your security software to control or monitor both Bluetooth pairing as well as the `Bluetooth File Exchange` application.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Internal Only - General

2.3.3.11 Ensure Computer Name Does Not Contain PII or Protected Organizational Information (Manual)

Profile Applicability:

- Level 2

Description:

If the computer is used in an organization that assigns host names, it is a good idea to change the computer name to the host name. This is more of a best practice than a security measure. If the host name and the computer name are the same, computer support may be able to track problems down more easily.

For organizations or for users that self-administer their own computers, it is important to not use sensitive or personal information in computer names. The name of a computer that uses untrusted networks will be exposed at a minimum to the responsible network team of that network. For instance, having your name as your `hostname` can provide useful knowledge to an attacker monitoring the network you may be connected to.

Examples of possibly inappropriate content in computer names include:

- User directory account names
- Computer directory account names where machine accounts exist
- Contact phone numbers
- Physical locations of offices or residences
- Personal information that can be augmented with Facebook data to assist social engineering attacks

Standard naming patterns avoid collisions and mitigate risk for computer users.

With mobile devices, using DHCP IP tracking has serious drawbacks. Hostname or computer name tracking makes much more sense for those organizations that can implement it. If the computer is using different names for the "Computer Name" DNS and Directory environments, it can be difficult to manage Macs in an Enterprise asset inventory.

Rationale:

Part of IT security is having visibility into all of the devices for which an organization is responsible. Without a complete inventory, it is impossible to ensure all security controls are met on all organizational devices.

Default macOS naming deconfliction controls can create issues for appropriate management and tracking as well as privacy exposure. By default, the name of a macOS computer is derived from the first user created. If the user has multiple computers or an image is used without an appropriate name change, there will be multiple computers with names derived from the same user for discovery deconfliction. How many "Ron Colvin's MacBook Pro" should there be, and are any missing?

Internal Only - General

Local network auto renaming to avoid collisions also allows for the enumeration of local computer names. Computers should not be named after their users, especially on untrusted networks. For social engineering purposes, the computer name should not provide a full name of the user or an identifiable name that might be used to assist in targeted user attacks.

A documented plan to better enable a complete device inventory without exposing user or organizational information is part of mature security.

Audit:

Graphical Method:

Perform the following steps to verify the computer name:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Verify that `Hostname` is set to your organization's parameters

Remediation:

Graphical Method:

Perform the following steps to set the computer name:

1. Open `System Settings`
2. Select `General`
3. Select `Sharing`
4. Select `Edit...`
5. Set `Hostname` to your organization's parameters

References:

1. https://support.apple.com/en-ca/guide/mac-help/mchlp1177/mac
2. https://uberagent.com/blog/choosing-macos-computer-names-wisely/
3. https://support.apple.com/en-ca/guide/mac-help/mchlp2322/mac

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.1 Establish and Maintain Detailed Enterprise Asset Inventory Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	●	●	●
v7	9.1 Associate Active Ports, Services and Protocols to Asset Inventory Associate active ports, services and protocols to the hardware assets in the asset inventory.		●	●

Internal Only - General

2.3.4 Time Machine

One of the most important IT Operational concerns is to ensure that information is protected against loss or tampering. The purpose of the IT devices is to process the data, after all. At one time the cost of IT equipment and the volume of the data might make protection of the equipment itself more important. At this point, the vast size of data archives and the lower cost of end-user equipment makes data protection central to operational planning. Backup strategies are generally focused on ensuring that there are multiple copies of relevant versions of user files. The plan is that no single hardware or software loss or failure will result in major data loss.

Apple does not provide a native remote logging capability that encrypts data in transit (DIT). If no third party tool or agent is installed on organizational-manned Macs, it is even more important to ensure that backup processes are implemented with log backups as part of the architecture.

In recent years the criticality of information backup, protection of data, and data backups has become even more important with the rise of cybercriminals that not only commit denial-of-service attacks using ransomware to encrypt your working data to make it inaccessible, but also encrypt the backups if reachable. Newer threats include blackmail to compromise data confidentiality. A comprehensive plan to protect data from compromise is even more vital with current threats. The Time Machine controls are only recommended best practices to assist in ease of frequent backups and the encryption of backup volumes.

Apple introduced Time Machine in 2007 as a simple-to-use, built-in mechanism for users to ensure that their machine was backed up, and if there was a mistake or loss, that information could be easily recovered. There are other solutions to ensure information is protected, including several Enterprise solutions and simple drive or directory cloning.

The controls in this section are specifically about Time Machine. The general ideas are applicable to any data backup solution. These controls are only pertinent to organizations already using Time Machine as part of their backup solutions to ensure the included Apple backup solution is being used effectively. We are not endorsing that Time Machine should be used exclusively or as part of the Enterprise backup solution. While your organization might not have explicitly allow or deny the use of Time Machine, users may still use Time Machine as a backup that is not controlled by IT. The controls first check that Time Machine is actually enabled.

To enable Time Machine, follow the instructions here: https://support.apple.com/en-us/HT201250

For more details on Time Machine:

- https://eclecticlight.co/tag/time-machine/
- https://www.pcmag.com/how-to/how-to-back-up-your-mac-with-time-machine

Internal Only - General

2.3.4.1 Ensure Backup Automatically is Enabled If Time Machine Is Enabled (Automated)

Profile Applicability:

- Level 2

Description:

Backup solutions are only effective if the backups run on a regular basis. The time to check for backups is before the hard drive fails or the computer goes missing. In order to simplify the user experience so that backups are more likely to occur, Time Machine should be on and set to Back Up Automatically whenever the target volume is available.

Operational staff should ensure that backups complete on a regular basis and the backups are tested to ensure that file restoration from backup is possible when needed.

Backup dates are available even when the target volume is not available in the Time Machine plist.

SnapshotDates = ("2020-08-20 12:10:22 +0000", "2021-02-03 23:43:22 +0000", "2022-02-19 21:37:21 +0000", "2023-02-22 13:07:25 +0000", "2024-08-20 14:07:14 +0000"

When the backup volume is connected to the computer, more extensive information is available through `tmutil`. See `man tmutil`.

Note: This recommendation needs to be set on devices where Time Machine is enabled. If Time Machine is disabled, the audit is passed by default.

Rationale:

Backups should automatically run whenever the backup drive is available.

Impact:

The backup will run periodically in the background and could have user impact while running.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure that automatic backups are set if Time Machine is enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Time Machine`
4. Verify that 'Next Back Up' is set to `Automatically`

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `AutoBackup=1`

Terminal Method:

Run the following command to verify that Time Machine is set to automatically backup if Time Machine is enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.TimeMachine')
\
  .objectForKey('AutoBackup'))
  if ( pref1  == null ) {
    return("Preference Not Set")
  }  else if ( pref1 == 1 ) {
    return("true")
  }  else {
    return("false")
  }
}
EOS
```

The output should either be `Preference Not Set` or `true`. If it is `false`, then the computer is not in compliance

Run the following command to check the snapshot dates to verify that the dates meet your organization's approved backup frequency:

```
% /usr/bin/sudo /usr/bin/defaults read
/Library/Preferences/com.apple.TimeMachine.plist Destinations
```

The output will contain all the Time Machine backups in the format `"YYYY-MM-DD HH:MM:SS +0000"`

Internal Only - General

example:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.TimeMachine')
\
  .objectForKey('AutoBackup'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.TimeMachine')
\
  .objectForKey('LastDestinationID'))
  if ( pref2  == null ) {
    return("Preference Not Set")
  }  else if ( pref1 == 1 ) {
    return("true")
  }  else {
    return("false")
  }
}
EOS

true

% /usr/bin/sudo /usr/bin/defaults read read
/Library/Preferences/com.apple.TimeMachine.plist Destinations

(
        {
        BackupAlias = {length = 348, bytes = 0x00000000 015c0002 00011442
61636b75 ... 20564d00 ffff0000 };
        BytesAvailable = 4855873536;
        BytesUsed = 5125054464;
        ConsistencyScanDate = "2022-09-22 18:21:01 +0000";
        DestinationID = "A64EA502-30DD-480C-9F7B-4F3EEDD0D186";
        DestinationUUIDs =         (
            "0D946E5D-68ED-4F63-BCBD-CE7FC94F47C0"
        );
        FilesystemTypeName = apfs;
        HealthCheckDecision = 0;
        InheritanceDecision = 0;
        LastKnownEncryptionState = Encrypted;
        RESULT = 0;
        ReferenceLocalSnapshotDate = "2024-09-22 18:21:53 +0000";
        SnapshotDates =         (
            "2024-09-22 18:21:01 +0000",
            "2024-09-22 18:21:32 +0000",
            "2024-09-22 18:21:57 +0000"
        );
    }
)
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to enable Time Machine automatic backup:

1. Open `System Settings`
2. Select `General`
3. Select `Time Machine`
4. Select `Options...`
5. Set `Back up frequency` to `Automatically <every hour/every day/every week>`

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.MCX.TimeMachine`
2. The key to include is `AutoBackup`
3. The key must be set to `<true/>`

Note: In previous versions of the benchmark, the plist could be set in `Terminal`. In macOS 15 Sequoia that plist is now protected and cannot be written to, so the command line remediation has been removed. Both the profile method and graphical method still configure Time Machine to the required state.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.2 Perform Automated Backups Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	●	●	●
v7	10.1 Ensure Regular Automated Back Ups Ensure that all system data is automatically backed up on regular basis.	●	●	●

Internal Only - General

2.3.4.2 Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

One of the most important security tools for data protection on macOS is FileVault. With encryption in place, it makes it difficult for an outside party to access your data if they get physical possession of the computer. One very large weakness in data protection with FileVault is the level of protection on backup volumes. If the internal drive is encrypted but the external backup volume that goes home in the same laptop bag is not, it is self-defeating. Apple tries to make this mistake easily avoided by providing a checkbox to enable encryption when setting up a Time Machine backup. Using this option does require some password management, particularly if a large drive is used with multiple computers. A unique, complex password to unlock the drive can be stored in keychains on multiple systems for ease of use.

While some portable drives may contain non-sensitive data and encryption may make interoperability with other systems difficult, backup volumes should be protected just like boot volumes.

Note: This recommendation needs to be set on devices where Time Machine is enabled. If Time Machine is disabled, the audit is passed by default.

Rationale:

Backup volumes need to be encrypted.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure the drive used for Time Machine is encrypted:

1. Open `System Settings`
2. Select `General`
3. Select `Time Machine`
4. Verify that every drive setup for Time Machine states `Encrypted`

Terminal Method:

Run the following command to verify if the Time Machine disk encryption is enabled:

```
% /usr/bin/sudo /usr/bin/defaults read
/Library/Preferences/com.apple.TimeMachine.plist | grep -c NotEncrypted

0
```

Remediation:

Graphical Method:

Perform the following steps to enable encryption on the Time Machine drive:

1. Open `System Settings`
2. Select `General`
3. Select `Time Machine`
4. Select the unencrypted drive
5. Select `-` to forget that drive as a destination
6. Select `+` to add a different drive as the destination
7. Select `Set Up Disk...`
8. Set `Encrypt Backup` to enabled
9. Enter a password in the `New Password` and the same password in the `Re-enter Password` fields
10. A password hint is required, but it is recommended that you do not use any identifying information for the password

Note: In macOS 12.0 Monterey and previous, the existing Time Machine drive could have encryption added without formatting it. This is no longer possible in macOS 13.0 Ventura. If you wish to keep previous backups from the unencrypted volume, you will need to manually move those files over to the new encrypted drive.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v8	11.3 Protect Recovery Data Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	●	●	●
v7	10.4 Ensure Protection of Backups Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

Internal Only - General

2.4 Menu Bar

The `Menu Bar System Settings` pane allows modification to `Control Center` modules and what is displayed in the `menu bar`.

Many `menu bar` icons provide additional status information when the option key is selected along with the menu, including WiFi and Bluetooth.

Internal Only - General

2.4.1 Audit Menu Bar and Control Center Icons (Manual)

Profile Applicability:

- Level 1

Description:

The Menu Bar is the horizontal strip that runs across the very top of your Mac's screen. The Control Center is a panel that groups the most frequently used system settings into one convenient location, similar to Control Center on an iPhone or iPad.

Rationale:

The presence of an unfamiliar or persistent icon, especially those indicating active sensors when you are not actively using an app that needs them, ex: the orange/green/purple dots for microphone, camera, or system audio. Inconsiderate application vendors may insert an icon in the menu bar on application install without user interaction.

Impact:

There should be no impact on the user.

Audit:

Graphical Method:

Perform the following steps to verify Menu Bar and Control Center icons:

1. Open `System Settings`
2. Select `Menu Bar`
3. Verify that all items listed in the `Allow in the menu bar` section are allowed by your organization
4. Select the `Control Center` icon in the menu bar
5. Verify that the `Control Center` options meet your organization's requirements

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to set (or remove) Menu Bar and Control Center icons:

1. Open `System Settings`
2. Select `Menu Bar`
3. Remove any items in `Allow in the menu bar` section are not allowed by your organization

Note: If there are unrecognized applications in the `Allow in the Menu Bar` section, this is a finding and should be investigated.

4. Select the `Control Center` icon in the menu bar
5. Set the `Control Center` options to meet your organization's requirements

Note: If there are unrecognized settings in `Control Center`, this is a finding and should be investigated.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	15.4 Disable Wireless Access on Devices if Not Required Disable wireless access on devices that do not have a business purpose for wireless access.			●
v7	15.5 Limit Wireless Access on Client Devices Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

Internal Only - General

2.5 Apple Intelligence & Siri

Internal Only - General

2.5.1 Apple Intelligence

The security recommendations provided are based on the assumption that an organization utilizes AI-powered products. A trust relationship with the technology vendor is essential, as sensitive data may be stored on their servers, similar to email and cloud storage. However, some features of the AI model also require the level of trust between customers of the AI model. If your data is used to train the AI model, then the other customers of the AI model can receive guidance that could be based on your organization's data. Enabling any AI feature(s) should be driven by organizational requirements.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended settings or disabling the feature(s) based on organizational needs.

Note: Ensure proprietary data is not used for AI model training to prevent data leaks.

For more information about Apple Intelligence view these links:

- Apple Intelligence Information Page
- Private Cloud Compute Security Guide
- Virtual Research Environment
- Apple PCC Source Code Git Repository
- Introducing Apple's On-Device and Server Foundation Models
- Apple Intelligence & Privacy
- Privacy Governance
- Apple Differential Privacy White Paper
- Understanding Aggregate Trends for Apple Intelligence Using Differential Privacy

To learn more about controlling Apple Intelligence in your organization:

- Raising Your IQ on Apple Intelligence
- From Smart to Smarter: Elevating Apple IQ Even More

Internal Only - General

2.5.1.1 Ensure External Intelligence Extensions Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The `External Intelligence Extensions` allows Apple Intelligence to interface with 3rd part generative AI tools. Apple's external intelligence extension represents a calculated risk. They are extending their on-device privacy and security model to the cloud with PCC (Private Cloud Compute), and then carefully integrating with a third-party AI like ChatGPT, emphasizing user consent, data minimization, and strong contractual obligations. However, the inherent nature of sending data to an external service means a degree of trust is placed on that third party's security posture and adherence to agreements. However, sending data to an external service is additional risk that must be reviewed and accepted in an organizational security plan.

Rationale:

While Apple has put significant effort into designing Apple Intelligence with a privacy-first approach, the external intelligence extension introduces legitimate security risks that might lead an individual or organization to disable it.

Impact:

The user would lose the ability to use Apple Intelligence to compose completely new text or access a broader range of resources directly within your apps. You could not use Siri or the Writing Tools to draft a complex email from scratch or generate creative content that goes beyond on-device capabilities but would need to use separate third-party AI providers.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify that 3rd party integrations in Apple Intelligence is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow External Intelligence Extensions` set to `False`
5. Verify that an installed profile has `Allow External Intelligence Sign-In` set to `False`

Terminal Method:

Run the following command to verify that a profile is installed that disables 3rd party integration in Apple Intelligence:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowExternalIntelligenceIntegrations').js
EOS

false

% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowExternalIntelligenceIntegrationsSignIn').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowExternalIntelligenceIntegrations`
3. The key must be set to `<false/>`
4. The second key to include is `allowExternalIntelligenceIntegrationsSignIn`
5. The key must be set to `<false/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.5.1.2 Ensure Writing Tools Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple Intelligence Writing Tools are a suite of AI-powered features integrated across iOS, iPadOS, and macOS, enabling users to enhance their text by proofreading for errors, rewriting content to adjust tone or style, summarizing lengthy passages into concise forms, and even composing new text from scratch. While many of these functions process securely on-device, there is the possibility of leveraging Apple's private cloud infrastructure.

Rationale:

The core of the security argument for disabling Apple Intelligence's Writing Tools revolves around unacceptable risk exposure to third parties and the potential for unintended data leakage. For individuals or organizations handling sensitive, confidential, or regulated data, the perceived risks of third-party exposure, potential for accidental data leakage, and compliance challenges often outweigh the convenience benefits. Disabling this feature is a rational and proactive security measure.

Impact:

Disabling Apple Intelligence's Writing Tools means you could reduce convenience and efficiency for writing, forcing you to do these tasks manually. However, it also enhances security and privacy by preventing any text from potentially being sent off-device.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify that writing tools in Apple Intelligence is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow Writing Tools` set to `False`

Terminal Method:

Run the following command to verify that a profile is installed that disables writing tools in Apple Intelligence:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowWritingTools').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowWritingTools`
3. The key must be set to `<false/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.5.1.3 Ensure Mail Summarization Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple Intelligence's Mail summarization feature uses AI to quickly condense long emails or entire email threads into a few key sentences or bullet points. It automatically appears as a short summary under emails in your inbox, or you can manually tap a "Summarize" button within an open email to get a more detailed overview of complex messages and conversations, helping you grasp the main points at a glance without reading everything.

Rationale:

If there's any concern that your sensitive email content, even if for summarization, might potentially be routed to this third-party service (even with consent prompts), or if you want to avoid any possibility of Apple's servers processing data from highly confidential communications (even within PCC's strong safeguards), disabling the feature ensures your mail content is processed via approved organizational services and on managed devices. This prioritizes absolute control and minimizes any external processing risk for highly sensitive information.

Impact:

The user will no longer see automatic short summaries beneath emails or have the option to generate them on demand.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify that mail summarization in Apple Intelligence is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow Mail Summary` set to `False`

Terminal Method:

Run the following command to verify that a profile is installed that disables mail summarization in Apple Intelligence:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowMailSummary').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowMailSummary`
3. The key must be set to `<false/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.5.1.4 Ensure Notes Summarization Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple Intelligence's Notes summarization feature quickly condenses content within the Notes app. This includes summarizing written text you've highlighted or, notably, automatically generating summaries from audio recordings taken directly within Notes, like lectures or meetings, helping you grasp key information at a glance.

Rationale:

Disabling Notes summarization is wise for security if your audio recordings or notes contain very private or sensitive information. While Apple usually keeps your data secure, turning this off ensures none of that sensitive content, especially from transcribed audio, ever leaves your device for any AI processing, giving you maximum control over your confidential data.

Impact:

If you disable Apple Intelligence's Notes summarization feature, the main impact is that the user will not get automatic or on-demand summaries of your written notes or audio recordings.

Audit:

Graphical Method:

Perform the following steps to verify that notes summarization in Apple Intelligence is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow Notes Transcription` set to `False`
5. Verify that an installed profile has `Allow Notes Transcription Summary` set to `False`

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that disables notes summarization in Apple Intelligence:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowNotesTranscription').js
EOS

false

% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowNotesTranscriptionSummary').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowNotesTranscription`
3. The key must be set to `<false/>`
4. The second key to include is `allowNotesTranscriptionSummary`
5. The key must be set to `<false/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.5.2 Siri

Internal Only - General

2.5.2.1 Ensure Siri Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

With macOS 10.12 Sierra, Apple has introduced Siri from iOS to macOS. While there are data spillage concerns with the use of data-gathering personal assistant software, the risk here does not seem greater in sending queries to Apple through Siri than in sending search terms in a browser to Google or Microsoft. While it is possible that Siri will be used for local actions rather than Internet searches, Siri could, in theory, tell Apple about confidential Programs and Projects that should not be revealed. This appears to be a usage edge case.

In cases where sensitive or protected data is processed and Siri could expose that information through assisting a user in navigating their machine, it should be disabled. Siri does need to phone home to Apple, so it should not be available from air-gapped networks as part of its requirements.

Most of the use case data published has shown that Siri is a tremendous time saver on iOS where multiple screens and menus need to be navigated through. Information like sports scores, weather, movie times, and simple to-do items on existing calendars can be easily found with Siri. None of the standard use cases should be more risky than already approved activity.

For information on Apple's privacy policy for Siri, click here.

Rationale:

Siri is being disabled because the listen for "Siri" or "Hey Siri" feature cannot be disabled globally or even through a user specific plist. Due to this, there is no guarantee that Listen for is disabled and therefore the mic is live and capturing everything around it.

Impact:

With Siri is disabled, a user loses the ability to perform hands-free tasks, get quick information, and control their device using voice commands.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify Siri settings:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow Assistant` is to `False`

Terminal Method:

Run the following command to verify that a profile is installed that sets Siri to your organization's setting:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAssistant').js
EOS

false
```

Note: Previously the benchmark would pass using the `com.apple.ironwood.support` profile payload. That is a deprecated profile and now the `com.apple.applicationaccess` should be used.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowAssistant`
3. Set the key to `<false/>`

References:

1. https://support.apple.com/en-us/HT210657

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.5.2.2 Ensure Listen for (Siri) Is Disabled (Manual)

Profile Applicability:

- Level 1

Description:

macOS includes the Siri digital assistant and if enabled it is always listening in case it is needed. In Sonoma a user may choose either "Hey Siri" or either "Siri" and "Hey Siri." In either case, Siri is using the microphone at all times to listen for instructions and then can record questions once activated. In an organizational environment where people are talking and listening on video/voice calls, there are too many opportunities for unauthorized information disclosure to have a live microphone at all times. If Siri will be used it may be on, with "Listen for" Off and a keyboard shortcut selected.

Note: Currently this recommendation cannot be disabled either globally with a profile or individually with a plist change, but only through the GUI. Due to this, we are moving this recommendation to be manual (but still disabled) and disabling Siri until it is possible to disable Listen for through a non-GUI method.

Rationale:

In most environments there is too much unbounded risk of data spillage with a microphone always on, listening for instruction, and listening for questions if attention is obtained, relying on cloud compute to answer them. There are many examples of data leakage for technology in this space, and future vulnerabilities and bugs are certainly possible.

Impact:

Siri will not be available for hands-free usage, or not available at all if turned off completely.

Audit:

Graphical Method:

Perform the following steps to ensure that "Hey Siri" is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `VoiceTriggerUserEnabled` set to `0`

Internal Only - General

Terminal Method:

Run the following command to verify that "Hey Siri" is disabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.Siri')\
.objectForKey('VoiceTriggerUserEnabled').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Siri`
2. The key to include is set to `VoiceTriggerUserEnabled`
3. The key must be set to `<false/>`

Note: After testing, this profile will disable `Hey Siri` only for the first input but not additional inputs. This issues seems to only occur using the Apple Studio Display (and possibly the Pro Display XDR, but no testing has occurred with that device) and it is not the primary input source. We are going to continue testing, but this seems to be an edge case.

References:

1. https://support.apple.com/guide/mac-help/use-siri-mchl6b029310/mac#:~:text=Turn%20on%20Siri,may%20need%20to%20scroll%20down.)&text=On%20the%20right%2C%20turn%20on,already%20on%2C%20then%20click%20Enable.
2. https://clario.co/blog/is-siri-always-listening/
3. https://www.siriuserguide.com/how-to-use-siri-macos/

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6 Privacy & Security

This section contains recommendations for configurable options under the `Privacy & Security` panel.

Additional privacy preference information from Apple

If the computer is present in an area where there are privacy concerns or sensitive activity is taking place, the Mac should be configured appropriately for the sensitive area.

Camera: If the computer is present in an area where there are privacy concerns or sensitive activity is taking place, the camera should be covered at those times. A permanent cover or alteration may be required when the computer is always located in a confidential area.

Microphone: If the computer is present in an area where there are privacy concerns or sensitive activity is taking place, the microphone input should be set to zero in the input tab of the Sound preference pane at those times. Individual management of applications with access to the microphone may be managed in the Security & Privacy Preference Pane under Microphone.

WiFi and Bluetooth: Some organizations have comprehensive rules that cover the use of wireless technologies in order to implement operational security. There are often specific policies governing the use of both Bluetooth and Wi-Fi (802.11) that may include disabling the wireless capability in either software or hardware, or both. Wireless access is part of the feature set required for mobile computers and is considered essential for most users.

Malware is continuously discovered that circumvents the privacy controls of the built-in video, audio, or network capabilities. No computer has perfect security, and even if all the drivers are disabled or removed, working drivers can be reintroduced by a determined attacker. Additional info Apple Pays $100.5K Bug Bounty for Mac Webcam Hack

Mac users, update Zoom now — your microphone may be spying on you

Recommended settings for Wi-Fi routers and access points

Control access to the microphone on Mac

Bluetooth security

Internal Only - General

2.6.1 Location Services

Internal Only - General

2.6.1.1 Ensure Location Services Is Enabled (Automated)

Profile Applicability:

- Level 2

Description:

macOS uses location information gathered through local Wi-Fi networks to enable applications to supply relevant information to users. With the operating system verifying the location, users do not need to change the time or the time zone. The computer will change them based on the user's location. They do not need to specify their location for weather or travel times, and they will receive alerts on travel times to meetings and appointments where location information is supplied.

Location Services simplify some processes with mobile computers, such as asset management and time or log management.

There are some use cases where it is important that the computer not be able to report its exact location. While the general use case is to enable Location Services, it should not be allowed if the physical location of the computer and the user should not be public knowledge.

Rationale:

Location Services are helpful in most use cases and can simplify log and time management where computers change time zones.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to ensure that Location Services is enabled:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Location Services`
4. Verify `Location Services` is enabled

Terminal Method:

Run the following command to verify that Location Services are enabled:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -c com.apple.locationd

1

% /usr/bin/sudo -u _locationd /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.locationd').objectForKey(
'LocationServicesEnabled').js
EOS

true
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to enable Location Services:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Location Services`
4. Set `Location Services` to enabled

Terminal Method:

Run the following command to enable Location Services:

```
% /usr/bin/sudo /bin/launchctl load -w
/System/Library/LaunchDaemons/com.apple.locationd.plist
```

If the `com.apple.locationd.plist` outputs `0`, run the following command to also ensure Location Services is running:

```
% /usr/bin/sudo /usr/bin/defaults write
/var/db/locationd/Library/Preferences/ByHost/com.apple.locationd
LocationServicesEnabled -bool true

% /usr/bin/sudo /usr/bin/killall locationd
```

Note: In some use cases, organizations may not want Location Services running. To disable Location Services, run the command: `/usr/bin/sudo /usr/bin/defaults write /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd LocationServicesEnabled -bool false`

References:

1. https://support.apple.com/en-us/HT204690

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.6.1.2 Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled (Automated)

Profile Applicability:

- Level 2

Description:

This setting provides the user an understanding of the current status of Location Services and which applications are using it.

Rationale:

Apple has fully integrated location services into macOS. When user applications access location an arrow is displayed next to the Control Center in the menu bar to give users an indication when their location is being accessed. By default system services like time zones, weather, travel times, geolocation, "Find my Mac," and advertising services do not indicate the location is accessed.

Enabling the “Show location icon in the menu bar when System Services request your location” setting will show an arrow in the control center when a system service accesses the location. Although an indication that location was accessed, Control Center will only say that it was accessed by "System Services" and not the individual service. Looking in System Settings > Location Services > System Services > Details… will expose exactly which system services have accessed Location Services in the last 24 hours. Third-party tools will be shown individually when they access location services.

Impact:

Users may be provided visibility to a setting they cannot control if organizations control Location Services globally by policy.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify the settings for location services icon to be in the menu bar:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Location Services`
4. Select `Details...`
5. Verify `Show location icon in menu bar when System Services request your location` is set to `True`

Terminal Method:

Run the following commands to verify that the location services icon is in the menu bar:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.locationmenu')\
.objectForKey('ShowSystemServices').js
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to set whether the location services icon is in the menu bar:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Location Services`
4. Select `Details...`
5. Set `Show location icon in menu bar when System Services request your location` to enabled

Terminal Method:

Run the following commands to set the option of the location services icon being in the menu bar:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.locationmenu.plist ShowSystemServices -bool
true
```


Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.6.1.3 Audit Location Services Access (Manual)

Profile Applicability:

- Level 2

Description:

macOS uses location information gathered through local Wi-Fi networks to enable applications to supply relevant information to users. While Location Services may be very useful, it may not be desirable to allow all applications that can use Location Services to use your location for Internet queries in order to provide tailored content based on your current location.

Ensure applications that can use Location Services are authorized and provide that information where the application interacts with external systems. Apple offers feedback within System Preferences and may be enabled to supply information on the menu bar when Location Services are used.

Safari can deny access from websites or prompt for access.

Applications that support Location Services can be individually controlled in the Privacy tab in Security & Privacy under System Preferences.

Access should be evaluated to ensure that privacy controls are as expected.

Rationale:

Privacy controls should be monitored for appropriate settings.

Impact:

Many macOS features rely on Location Services for tailored information. Users expect their time zone and weather to be relevant to where they are without manual intervention. Find my Mac needs to know where your Mac is actually located. Where possible, the tolerance between location privacy and convenience may be best left to the user when the location itself is not sensitive. If facility locations are not public, location information should be tightly controlled.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify what applications are enabled for Location Services:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Location Services`
4. Verify that the applications allowed to access Location Services are set to your organization's requirements

Perform the following steps to verify what websites are enabled to ask for access to Location Services:

1. Open `Safari`
2. Select `Safari` from the `menu bar`
3. Select `Settings`
4. Select `Websites`
5. Select `Location`
6. Verify that `When visiting other websites` is set to your organization's requirements

Terminal Method:

Run the following command to evaluate the applications that are enabled to use Location Services:

```
% /usr/bin/sudo /usr/bin/defaults read /var/db/locationd/clients.plist
```

Ensure that all applications listed have been authorized to access location information.

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to disable unnecessary applications from accessing Location Services:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Location Services`
4. Set any applications listed to your organization's requirements

Perform the following steps to set websites to ask for permission to access Location Services:

1. Open `Safari`
2. Select `Safari` from the `menu bar`
3. Select `Settings`
4. Select `Websites`
5. Select `Location`
6. Set `When visiting other websites` to your organization's requirements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.6.2 Full Disk Access

Internal Only - General

2.6.2.1 Audit Full Disk Access for Applications (Manual)

Profile Applicability:

- Level 2

Description:

Starting with macOS 10.14 Mojave, Apple introduced Transparency, Consent, and Control (TCC) to enhance user privacy by requiring apps to get explicit permission before accessing sensitive data or system features. Full Disk Access (FDA) is a privacy category managed by the TCC (Transparency, Consent, and Control) framework. It controls whether applications can access certain protected areas of the file system, such as Mail, Messages, Safari data, and system logs.

Rationale:

Only applications from verified developers with a legitimate operational need—such as security monitoring or system management tools—should be granted Full Disk Access. The access and trust-worthiness of applications should be verified on a regular basis.

Impact:

Applications with Full Disk Access can access data from certain protected areas of the file system such as Mail, Messages, Safari data, and system logs.

Audit:

Graphical Method:

Perform the following steps to verify what applications have full disk access:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Full Disk Access`
4. Verify that the applications are set to your organization's requirements

Terminal Method:

Run the following command to verify that what applications have full disk access enabled:

```
% /usr/bin/sudo /usr/bin/sqlite3 /Library/Application\
Support/com.apple.TCC/TCC.db 'select client from access where auth_value and
service = "kTCCServiceSystemPolicyAllFiles"'
```

The output will be what applications have full disk access enabled.

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to set full disk access for applications that meet your organization's requirements:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Full Disk Access`
4. Set any listed applications to your organization's requirements
5. (Optional) Select the `+` to add applications to the list, or `-` to remove them

References:

1. https://support.apple.com/guide/security/controlling-app-access-to-files-secddd1d86a6/web
2. https://lapcatsoftware.com/articles/FullDiskAccess.html
3. https://www.techrepublic.com/article/secure-mac-data-full-disk-access/
4. https://support.intego.com/hc/en-us/articles/360016683471-Enable-Full-Disk-Access-in-macOS
5. https://jumpcloud.com/support/grant-full-disk-access-permissions-to-the-jumpcloud-agent-for-macos
6. https://docs.metallic.io/metallic/enabling_full_disk_access_for_macos.html
7. https://knowledge.broadcom.com/external/article/176368/configuring-mdm-profiles-for-full-disk-a.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	16.7 Use Standard Hardening Configuration Templates for Application Infrastructure Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.6.3 Analytics & Improvements

The settings contained within `Analytics & Improvements` are designed to help Apple and developers improve their products and services automatically. To do this, data is sent automatically to Apple (or app developers). Apple provides a mechanism to send diagnostic and analytics data back to Apple to help them improve the platform. Information sent to Apple may contain internal organizational information that should be controlled and not available for processing by Apple. This data may be shared with third-parties, and each recommendation in this sub-section deals with different type of data that is collected and shared.

Share Mac Analytics (Share with App Developers dependent on Mac Analytic sharing)

- Includes diagnostics, usage and location data

Share iCloud Analytics

- Includes iCloud data and usage information

To learn more about privacy at Apple, visit: www.apple.com/privacy

Internal Only - General

2.6.3.1 Ensure Share Mac Analytics Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Share Mac Analytics (Share with App Developers dependent on Mac Analytic sharing) includes diagnostics, usage, and location data. Turn off all Analytics and Improvements sharing.

Rationale:

Organizations should have knowledge of what is shared with the vendor and that this setting automatically forwards information to Apple.

Impact:

There should be no impact.

Audit:

Graphical Method:

Perform the following steps to verify that Mac analytics are not being send to Apple:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Also verify that an installed profile has `Auto Submit` set to `False`

Terminal Method:

Run the following command to verify that a profile is installed that disables sharing Mac analytics to Apple:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SubmitDiagInfo')\
.objectForKey('AutoSubmit').js
EOS

false
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.SubmitDiagInfo`
2. The key to include is `AutoSubmit`
3. The key must be set to `<false/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6.3.2 Ensure Improve Siri & Dictation Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

`Improve Siri & Dictation` allows Apple to store and review audio of your Siri and dictation interactions from the device. Turn off all Analytics and Improvements sharing.

Rationale:

Organizations should have knowledge of what is shared with the vendor and that this setting automatically forwards information to Apple.

Impact:

There should be no impact.

Audit:

Graphical Method:

Perform the following steps to verify that Siri and dictation is not being send to Apple:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Also verify that an installed profile has `Siri Data Sharing Opt-In Status` set to `2`

Terminal Method:

Run the following command to verify that a profile is installed that disables sharing Siri and dictations to Apple:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.assistant.support')\
.objectForKey('Siri Data Sharing Opt-In Status').js
EOS

2
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.assistant.support`
2. The key to include is `Siri Data Sharing Opt-In Status`
3. The key must be set to `<integer>2<integer/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6.3.3 Ensure Improve Assistive Voice Features Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

`Improve Assistive Voice` shares audio recordings and transcripts of Vocal Shortcuts and Voice Control interactions anonymously to Apple. These are recordings and transcripts from the user that are being submitted which may include PII or restricted organizational information. Sharing this kind of information with any 3rd party, including the platform vendor, needs to be risk evaluated and only allowed after review and approval based on your organization's policies.

Rationale:

Organizations should have knowledge of what is shared with the vendor and that this setting automatically forwards information to Apple.

Impact:

There should be no impact.

Audit:

Graphical Method:

Perform the following steps to verify that assistive voice features are not being sent to Apple:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `AXSAudioDonationSiriImprovementEnabled` set to `0`

Terminal Method:

Run the following command to verify a profile installed that are not sending assistive voice features to Apple:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.Accessibility')\
.objectForKey('AXSAudioDonationSiriImprovementEnabled').js
EOS

false
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Accessibility`
2. The key to include is `AXSAudioDonationSiriImprovementEnabled`
3. The key must be set to `<false/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6.3.4 Ensure 'Share with app developers' Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

`Share with app developers` allows Apple to share crash and usage data with app developers. Turn off all Analytics and Improvements sharing.

Rationale:

Organizations should have knowledge of what is shared with the vendor and that this setting automatically forwards information to Apple.

Impact:

There should be no impact.

Audit:

Graphical Method:

Perform the following steps to verify that diagnostic data is not being send to Apple:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Also verify that an installed profile has `Allow Diagnostic Submission` set to `False`

Terminal Method:

Run the following command to verify that a profile is installed that disables sharing app analytics to Apple and developers:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowDiagnosticSubmission').js
EOS

false
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowDiagnosticSubmission`
3. The key must be set to `<false/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6.3.5 Ensure Share iCloud Analytics Is Disabled (Manual)

Profile Applicability:

- Level 1

Description:

Share iCloud Analytics shares analytics of usage and data from your iCloud account to Apple to help improve its products and services (including Siri and other intelligent features). Turn off all Analytics and Improvements sharing.

This setting will not appear if the user is not signed into a personal Apple Account.

Rationale:

Organizations should have knowledge of what is shared with the vendor and that this setting automatically forwards information to Apple.

Impact:

There should be no impact.

Audit:

Graphical Method:

Perform the following steps to verify that iCloud Analytics is not being sent to Apple:

1. Open `System Settings`
2. Open `Privacy & Security`
3. Select `Analytics & Improvements`
4. Verify that `Share iCloud Analytics` is disabled

Remediation:

Graphical Method:

Perform the following steps to disable Siri and dictation not being sent to Apple:

1. Open `System Settings`
2. Open `Privacy & Security`
3. Select `Analytics & Improvements`
4. Verify that `Share iCloud Analytics` is disabled

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6.4 Ensure Limit Ad Tracking Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple provides a framework that allows advertisers to target Apple users and end-users with advertisements. While many people prefer to see advertising that is relevant to them and their interests, the detailed information that is collected, correlated, and available to advertisers in repositories via data mining is often disconcerting. This information is valuable to both advertisers and attackers, and has been used with other metadata to reveal users' identities.

Organizations should manage advertising settings on computers rather than allow users to configure the settings.

Apple Information

Ad tracking should be limited on 10.15 and prior.

Rationale:

Organizations should manage user privacy settings on managed devices to align with organizational policies and user data protection requirements.

Impact:

Uses will see generic advertising rather than targeted advertising. Apple warns that this will reduce the number of relevant ads.

Audit:

Graphical Method:

Perform the following steps to verify that limited ad tracking is set:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `allowApplePersonalizedAdvertising` set to `0`

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that enables Limit Ad Tracking:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowApplePersonalizedAdvertising').js
EOS

false
```

Note: Since the profile method sets a system-wide setting, the individual user audit and/or remediation has been removed. To be compliant, a profile must be installed for this recommendation. We have included the individual user information in the additional information section for reference only.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowApplePersonalizedAdvertising`
3. The key must be set to `<false/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6.5 Ensure Gatekeeper Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Gatekeeper is Apple's application that utilizes allowlisting to restrict downloaded applications from launching. It functions as a control to limit applications from unverified sources from running without authorization. In an update to Gatekeeper in macOS 13 Ventura, Gatekeeper checks every application on every launch, not just quarantined apps.

Rationale:

Disallowing unsigned software will reduce the risk of unauthorized or malicious applications from running on the system.

Audit:

Graphical Method:

Perform the following steps to ensure that Gatekeeper is enabled:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Verify that 'Allow apps downloaded from' is set to 'App Store and identified developers'

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Policies` set to `Enable`
5. Verify that an installed profile has `Identified Developers` set to `Allow`

Terminal Method:

Run the following command to verify that Gatekeeper is enabled:

```
% /usr/bin/sudo /usr/sbin/spctl --status

assessments enabled
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to enable Gatekeeper:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Set 'Allow apps downloaded from' to 'App Store and identified developers'

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.systempolicy.control`
2. The key to include is `AllowIdentifiedDevelopers`
3. The key must be set to `<true/>`
4. The key to also include is `EnableAssessment`
5. The key must be set to `<true/>`

Note: In previous versions of macOS, Gatekeeper could be set using the binary. This has been removed in macOS 15 Sequoia.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●

Internal Only - General

2.6.6 Ensure FileVault Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

FileVault secures a system's data by automatically encrypting its boot volume and requiring a password or recovery key to access it.

FileVault should be used with a saved escrow key to ensure that the owner can decrypt their data if the password is lost.

FileVault may also be enabled using command line using the `fdesetup` command. To use this functionality, consult the Der Flounder blog for more details (see link below under References).

Rationale:

Encrypting sensitive data minimizes the likelihood of unauthorized users gaining access to it.

Impact:

Mounting a FileVault encrypted volume from an alternate boot source will require a valid password to decrypt it. Apple has also implemented an escalating policy for failed passwords. To find out more about that, read here: Passcodes and passwords

Audit:

Graphical Method:

Perform the following steps to verify that FileVault is enabled:

1. Open `System Settings`
2. Select `Privacy & Privacy`
3. Verify that `FileVault` states `FileVault is turned on for the disk "<disk name>"`
4. Select `General`
5. Select `Device Management`
6. Verify that an installed profile has `FileVault Can't Disable` set to `True`

Internal Only - General

Terminal Method:

Run the following command to verify that FileVault is enabled and cannot be disabled:

```
% /usr/bin/sudo /usr/bin/fdesetup status

FileVault is On

$ /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('dontAllowFDEDisable').js
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to enable FileVault:

1. Open `System Settings`
2. Select `Security & Privacy`
3. Select `Turn On...`

Note: This will allow you to create a recovery key for FileVault. As of macOS 26 Tahoe, the recovery key can be requested on demand for macOS devices that are not connected to an MDM.

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.MCX`
2. The key to include is `dontAllowFDEDisable`
3. The key must be set to `<true/>`

Note: This profile is required to pass the audit.

References:

1. https://derflounder.wordpress.com/2015/02/02/managing-yosemites-filevault-2-with-fdesetup/
2. https://derflounder.wordpress.com/2019/01/15/unlock-or-decrypt-your-filevault-encrypted-boot-drive-from-the-command-line-on-macos-mojave/
3. https://derflounder.wordpress.com/2021/10/29/use-of-filevault-institutional-recovery-keys-no-longer-recommended-by-apple/
4. https://support.apple.com/guide/security/passcodes-and-passwords-sec20230a10d/1/web/1

Internal Only - General

Additional Information:

FileVault may not be desirable on a virtual OS. As long as the hypervisor and file storage are encrypted, the virtual OS does not need to be. Rather than checking if the OS is virtual and passing the control regardless of the encryption of the host system, the normal check will be run. Security officials can evaluate the comprehensive controls outside of the OS being tested.

Part of FileVault management in an Enterprise environment is to ensure key management if technical staff need to decrypt encrypted volumes. More information here: https://derflounder.wordpress.com/2021/10/29/use-of-filevault-institutional-recovery-keys-no-longer-recommended-by-apple/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

Internal Only - General

2.6.7 Audit Lockdown Mode (Manual)

Profile Applicability:

- Level 2

Description:

Apple introduced Lockdown Mode as a security feature in their 2022 OS releases that provides additional security protection Apple describes as *extreme*. Users and organizations that suspect some users are targets of advanced attacks must consider using this control.

When lockdown mode is enabled, specific trusted websites can be excluded from Lockdown protection if necessary.

Rationale:

Lockdown Mode was designed by Apple as an aggressive approach to commonly attacked OS features where additional controls could reduce the attack surface. IT systems and devices, including their users, are subject to continuous exploit attempts. Most of that activity is not from an advanced attacker and can be considered background noise to a patched, hardened device. Advanced attackers are of more concern and a risk review to understand organizational targets and use Lockdown Mode where appropriate is necessary.

Impact:

Lockdown Mode must be tested appropriately for real-world impact on users prior to use. As a new feature there is not sufficient technical reporting on user impacts.

Audit:

Graphical Method:

Perform the following steps to verify the settings for Lockdown Mode:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Verify `Lockdown Mode` is set to your organization's requirements

Internal Only - General

Terminal Method:

Run the following command to verify that Lockdown mode is enabled for the user:

```
$ /usr/bin/sudo -u <username> /usr/bin/defaults read .GlobalPreferences.plist
LDMGlobalEnabled 2>/dev/null
```

When Lockdown mode has been enabled, it will return `1` and when disabled return `0`. If Lockdown has never been enabled, it will return no value.

NOTE: Lockdown mode is set per local user, therefore you must iterate through each local user to verify the settings.

Remediation:

Graphical Method:

Perform the following steps to set Lockdown Mode to your organization's requirements:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Set `Lockdown Mode` to your organization's requirements

References:

1. https://support.apple.com/en-us/HT212650
2. https://www.lifewire.com/use-lockdown-mode-on-mac-6454923

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

Internal Only - General

2.6.8 Ensure an Administrator Password Is Required to Access System-Wide Preferences (Automated)

Profile Applicability:

- Level 1

Description:

System Preferences controls system and user settings on a macOS Computer. System Preferences allows the user to tailor their experience on the computer as well as allowing the System Administrator to configure global security settings. Some of the settings should only be altered by the person responsible for the computer.

Rationale:

By requiring a password to unlock system-wide System Preferences, the risk of a user changing configurations that affect the entire system is mitigated and requires an admin user to re-authenticate to make changes.

Impact:

Users will need to enter their password to unlock some additional preference panes that are unlocked by default like Network, Startup and Printers & Scanners.

Audit:

Graphical Method:

Perform the following steps to verify that an administrator password is required to access system-wide preferences:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Advanced`
4. Verify that `Require an administrator password to access system-wide settings` is enabled

Internal Only - General

Terminal Method:

Run the following command to verify that accessing system-wide preferences requires an administrator password:

```
% authDBs=("system.preferences" "system.preferences.energysaver"
"system.preferences.network" "system.preferences.printing"
"system.preferences.sharing" "system.preferences.softwareupdate"
"system.preferences.startupdisk" "system.preferences.timemachine")
  result="1"
  for section in ${authDBs[@]}; do
    if [[ $(/usr/bin/security -q authorizationdb read "$section" |
/usr/bin/xmllint -xpath 'name(//*[contains(text(), "shared")]/following-
sibling::*[1])' -) != "false" ]]; then
      result="0"
    fi
    if [[ $(security -q authorizationdb read "$section" | /usr/bin/xmllint -
xpath '//*[contains(text(), "group")]/following-sibling::*[1]/text()' - ) !=
"admin" ]]; then
      result="0"
    fi
    if [[ $(/usr/bin/security -q authorizationdb read "$section" |
/usr/bin/xmllint -xpath 'name(//*[contains(text(), "authenticate-
user")]/following-sibling::*[1])' -) != "true" ]]; then
      result="0"
    fi
    if [[ $(/usr/bin/security -q authorizationdb read "$section" |
/usr/bin/xmllint -xpath 'name(//*[contains(text(), "session-
owner")]/following-sibling::*[1])' -) != "false" ]]; then
      result="0"
    fi
  done
  echo $result
```

Note: Every audit and remediation includes `sudo` before all commands. This is an exception because `authdb` is a variable and using `sudo` causes an error in the output.

Remediation:

Graphical Method:

Perform the following steps to verify that an administrator password is required to access system-wide preferences:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Advanced`
4. Set `Require an administrator password to access system-wide settings` to enabled

Internal Only - General

Terminal Method:

The authorizationdb settings cannot be written to directly, so the plist must be exported out to a temporary file. Changes can be made to the temporary plist, then imported back into the authorizationdb settings.

Run the following commands to enable that an administrator password is required to access system-wide preferences:

```
% authDBs=("system.preferences" "system.preferences.energysaver"
"system.preferences.network" "system.preferences.printing"
"system.preferences.sharing" "system.preferences.softwareupdate"
"system.preferences.startupdisk" "system.preferences.timemachine")

  for section in ${authDBs[@]}; do
    /usr/bin/security -q authorizationdb read "$section" >
"/tmp/$section.plist"

    class_key_value=$(usr/libexec/PlistBuddy -c "Print :class"
"/tmp/$section.plist" 2>&1)
    if [[ "$class_key_value" == *"Does Not Exist"* ]]; then
      /usr/libexec/PlistBuddy -c "Add :class string user"
"/tmp/$section.plist"
    else
      /usr/libexec/PlistBuddy -c "Set :class user" "/tmp/$section.plist"
    fi

    key_value=$(/usr/libexec/PlistBuddy -c "Print :shared"
"/tmp/$section.plist" 2>&1)
    if [[ "$key_value" == *"Does Not Exist"* ]]; then
      /usr/libexec/PlistBuddy -c "Add :shared bool false"
"/tmp/$section.plist"
    else
      /usr/libexec/PlistBuddy -c "Set :shared false" "/tmp/$section.plist"
    fi

    auth_user_key=$(/usr/libexec/PlistBuddy -c "Print :authenticate-user"
"/tmp/$section.plist" 2>&1)
    if [[ "$auth_user_key" == *"Does Not Exist"* ]]; then
      /usr/libexec/PlistBuddy -c "Add :authenticate-user bool true"
"/tmp/$section.plist"
    else
      /usr/libexec/PlistBuddy -c "Set :authenticate-user true"
"/tmp/$section.plist"
    fi
```


Internal Only - General

```
    session_owner_key=$(/usr/libexec/PlistBuddy -c "Print :session-owner"
"/tmp/$section.plist" 2>&1)
    if [[ "$session_owner_key" == *"Does Not Exist"* ]]; then
      /usr/libexec/PlistBuddy -c "Add :session-owner bool false"
"/tmp/$section.plist"
    else
      /usr/libexec/PlistBuddy -c "Set :session-owner false"
"/tmp/$section.plist"
    fi

    group_key=$(usr/libexec/PlistBuddy -c "Print :group"
"/tmp/$section.plist" 2>&1)
    if [[ "$group_key" == *"Does Not Exist"* ]]; then
      /usr/libexec/PlistBuddy -c "Add :group string admin"
"/tmp/$section.plist"
    else
      /usr/libexec/PlistBuddy -c "Set :group admin" "/tmp/$section.plist"
    fi

    /usr/bin/security -q authorizationdb write "$section" <
"/tmp/$section.plist"
  done
```

Note: Every audit and remediation includes `sudo` before all commands. This is an exception because `authdb` is a variable and using `sudo` causes an error in the output.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.7 Desktop & Dock

Internal Only - General

2.7.1 Ensure Screen Saver Corners Are Secure (Automated)

Profile Applicability:

- Level 2

Description:

Hot Corners can be configured to disable the screen saver by moving the mouse cursor to a corner of the screen.

Rationale:

Setting a hot corner to disable the screen saver poses a potential security risk since an unauthorized person could use this to bypass the login screen and gain access to the system.

Audit:

Graphical Method:

Perform the following steps to ensure that a Hot Corner is not set to Disable Screen Saver:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `<wvous-tl-corner>`, `<wvous-bl-corner>`, `<wvous-tr-corner>`, and `<wvous-br-corner>` is not set to `6`

Terminal Method:

Run the following command to verify that a profile is installed secures screen saver corners:

```
% /usr/bin/profiles -P -o stdout | /usr/bin/grep -Ec '"wvous-bl-corner" =
6|"wvous-br-corner" = 6|"wvous-tl-corner" = 6|"wvous-tr-corner" = 6'

0
```

Note: Since the profile method sets a system-wide setting, the individual user audit and/or remediation has been removed. To be compliant, a profile must be installed for this recommendation. We have included the individual user information in the additional information section for reference only.

Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.dock`
2. The key to include is `Forced`
3. The key must be set to the following:

```
<array>
        <dict>
                <key>mcx_preference_settings</key>
                        <dict>
                                <key>wvous-bl-corner</key>
                                <integer><≠6></integer>
                                <key>wvous-br-corner</key>
                                <integer><≠6></integer>
                                <key>wvous-tl-corner</key>
                                <integer><≠6></integer>
                                <key>wvous-tr-corner</key>
                                <integer><≠6></integer>
                        </dict>
                </dict>
</array>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

2.7.2 Audit iPhone Mirroring (Manual)

Profile Applicability:

- Level 2

Description:

`iPhone Mirroring` is a new feature offered in iOS 18 and macOS 15.0 Sequoia. It allows a macOS device to remotely access an iOS device connected to the same Apple Account. If a user has different Apple Accounts signed into iOS and macOS (ex. a managed Apple Account on macOS and a personal Apple Account on iOS), the feature is not available.

Rationale:

Enabling `iPhone Mirroring` may allow a macOS device to capture data from an iOS device (ex Image Capture). This would occur where the macOS device has not been approved to access that information by your organization's policies and the iOS device has been approved (or vice-versa).

If `iPhone Mirroring` is currently in use on an iOS device, the lock screen will have a notification that states `iPhone in Use` and state what device is using it. If `iPhone Mirroring` was in use on an iOS device but is no longer in use, the first time the user unlocks the iOS device it will notify the user that `iPhone was used from Mac`.

Impact:

If `iPhone Mirroring` is disabled, it would stop a user from accessing information on their iOS device while using their macOS device.

Audit:

Perform the following to if the system is configured for iPhone Mirroring:

Graphical Method:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Allow iPhone Mirroring` set to `True` or `False` based on your organization's requirements

Internal Only - General

Terminal Method:

Run the following command to verify the configuration for iPhone mirroring:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple. applicationaccess')\
.objectForKey('allowiPhoneMirroring').js
EOS
```

The output will be either true, allow iPhone mirroring, or false, disable iPhone mirroring.

Remediation:

Perform the following to configure iPhone Mirroring:

Graphical Method:

1. Open `System Settings`
2. Select `Desktop & Dock`
3. Under the `Widgets` sub-header, verify `iPhone` is configured to your organization's requirements

Note: The `iPhone` setting will only show up if there are multiple iPhones being connected to the user's Apple Account and setup with iPhone mirroring.

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowiPhoneMirroring`
3. The key must be set to either `<true/>` or `<false/>` depending on your organization's requirements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

Internal Only - General

2.8 Displays

Internal Only - General

2.8.1 Audit Universal Control Settings (Manual)

Profile Applicability:

- Level 1

Description:

Universal Control is an Apple feature that allows Mac users to control multiple other Macs and iPads with the same keyboard, mouse, and trackpad using the same Apple Account. The technology relies on already available iCloud services, particularly Handoff.

Universal Control simplifies the use of iCloud connectivity of multiple computers using the same Apple Account. This may simplify data transfer from organizationally-managed and personal devices. The use of the same iCloud account and Handoff is the underlying concern that should be evaluated. The use of the same keyboard or mouse across multiple devices does not by itself decrease organizational security.

Universal Clipboard, a feature of Universal Control, allows any device using the same Apple Account to access the clipboard of any other devices using the same Apple Account.

Rationale:

The use of devices together when some are organizational and some are not may complicate device management standards.

Universal control settings may also enable a user to share their clipboard across multiple devices authenticated to the same Apple Account, so disabling that should be discussed by the organization.

Impact:

The user should not be impacted if Universal Control is set either way.

Audit:

Graphical Method:

Perform the following steps to verify a profile is installed that configures Universal Control:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has with `com.apple.universalcontrol` in `Settings` and has `Disable` set to your organization's parameters.

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that sets Universal Control to your organization's parameters:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.universalcontrol')\
.objectForKey('Disable').js
EOS
```

If the output is `true`, Universal Control is disabled. If it is `false`, then Universal Control is enabled.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.universalcontrol`
2. The key to include is `Disable`
3. Set the key to `<true/>` or `<false/>` based on your organization's requirements

Note: Since the profile method sets a system-wide setting and not a user-level one, the profile method is the preferred method. It is always better to set system-wide than per user.

Note: If your organization is allowing Universal Control, your organization can still disable Universal Clipboard via a profile. To disable Universal Clipboard, create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.coreservices.useractivityd`
2. The key to include is `ClipboardSharingEnabled`
3. Set the key to `<false/>`

References:

1. https://support.apple.com/en-us/HT212757
2. https://support.apple.com/en-us/102459

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.9 Spotlight

This section is for Spotlight.

Internal Only - General

2.9.1 Ensure Help Apple Improve Search Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple provides a mechanism to send diagnostic and analytics data back to Apple to help them improve the platform. Information sent to Apple may contain internal organizational information that should be controlled and not available for processing by Apple.

Rationale:

Organizations should have knowledge of what is shared with the vendor and the setting automatically forwards information to Apple.

Impact:

There is no impact on the user, but metadata from search results would not be shared with Apple to improve search capability.

Audit:

Graphical Method:

Perform the following steps to ensure that Help Apple Improve Search is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Search Queries Data Sharing Status` set to `2`

Terminal Method:

Run the following command to verify that Help Apple Improve Search is disabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.assistant.support')\
.objectForKey('Search Queries Data Sharing Status').js
EOS

2
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.assistant.support`
2. The key to include is set to `Search Queries Data Sharing Status`
3. The key must be set to `<integer>2</integer>`

Default Value:

Help Apple to Improve Search is switched on. 'Search Queries Data Sharing Status' has a value of `1` or is not present.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

Internal Only - General

2.10 Battery (Energy Saver)

This section is for energy use controls. Prior to Big Sur (Mac OS 11) it was known only as `Energy Saver`.

On desktop Macs, this preference pane is still named `Energy Saver` and not `Battery`.

[Mac Energy Saver preferences explained]

Internal Only - General

2.10.1 OS Resuming From Sleep

In order to use a computer with Full Disk Encryption (FDE), macOS must keep encryption keys in memory to allow the use of the disk that has been FileVault protected. The storage volume has been unlocked and acts as if it were not encrypted. When the system is not in use, the volume is protected through encryption. When the system is sleeping and available to quickly resume, the encryption keys remain in memory.

If an unauthorized party has possession of the computer and the computer is only slept, there are known attack vectors that can be attempted against the RAM that has the encryption keys or the running operating system protected by a login screen. Network attacks if network interfaces are on, as well as USB or other open device ports, are possible. Most of these attacks require knowledge of unpatched vulnerabilities or a high level of sophistication if all the other controls function as intended.

There is little impact on hibernating the system rather than sleeping after an appropriate time period to remediate the risk of OS level attacks. Hibernation writes the keys to disk and requires FileVault to be unlocked prior to the OS being available. In the case of unauthorized personnel with access to the computer, encryption would have to be broken prior to attacking the operating system in order to recover data from the system.

Internal Only - General

2.10.1.1 Ensure the OS Is Not Active When Resuming from Standby (Intel) (Manual)

Profile Applicability:

- Level 2

Description:

In order to use a computer with Full Disk Encryption (FDE), macOS must keep encryption keys in memory to allow the use of the disk that has been FileVault protected. The storage volume has been unlocked and acts as if it were not encrypted. When the system is not in use, the volume is protected through encryption. When the system is sleeping and available to quickly resume, the encryption keys remain in memory.

https://www.helpnetsecurity.com/2018/08/20/laptop-sleep-security/

Mac systems should be set to hibernate after sleeping for a risk-acceptable time period. The default value for "standbydelay" is three hours (10800 seconds). This value is likely appropriate for most desktops. If Mac desktops are deployed in unmonitored, less physically secure areas with confidential data, this value might be adjusted. The desktop would have to retain power, however, so that the running OS or physical RAM could be attacked.

MacBooks should be set so that the standbydelay is 15 minutes (900 seconds) or less. This setting should allow laptop users in most cases to stay within physically secured areas while going to a conference room, auditorium, or other internal location without having to unlock the encryption. When the user goes home at night, the laptop will auto-hibernate after 15 minutes and require the FileVault password to unlock prior to logging back into the system when it resumes.

MacBooks should also be set to a hibernate mode that removes power from the RAM. This will stop the possibility of cold boot attacks on the system.

Macs running Apple silicon chips, rather than Intel chips, do not require the same configuration as Intel-based Macs.

Rationale:

To mitigate the risk of data loss, the system should power down and lock the encrypted drive after a specified time. Laptops should hibernate 15 minutes or less after sleeping.

Impact:

The laptop will take additional time to resume normal operation if only sleeping rather than hibernating.

Setting `hibernatemode` to `25` will disable the "always-on" feature of the Apple Silicon Macs.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify the hibernation settings and that FileVault keys are destroyed on standby:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPHardwareDataType | /usr/bin/grep
-e MacBook
```

If there is an output, run the following:

```
% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep -e standby
```

The output should include a `standbydelaylow` value ≤ 900, a `standbydelayhigh` value ≤ 900, and a `highstandbythreshold` value ≥ 90.

```
% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep hibernatemode

 hibernatemode        25
```

example:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPHardwareDataType | /usr/bin/grep
-e MacBook

      Model Name: MacBook Pro
      Model Identifier: MacBookPro13,1

% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep -e standby

 standbydelaylow      600
 standby              1
 standbydelayhigh     600
 highstandbythreshold 50

% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep hibernatemode

 hibernatemode        25
```

Note: To verify if you are running an Intel processor, run `/usr/sbin/sysctl -n machdep.cpu.brand_string`. The output will include `Intel`.

Internal Only - General

Remediation:

Terminal Method:

Run the following command to set the hibernate delays and to ensure the FileVault keys are set to be destroyed on standby:

```
% /usr/bin/sudo /usr/bin/pmset -a standbydelaylow <value≤900>
% /usr/bin/sudo /usr/bin/pmset -a standbydelayhigh <value≤900>
% /usr/bin/sudo /usr/bin/pmset -a highstandbythreshold <value≥90>
% /usr/bin/sudo /usr/bin/pmset -a destroyfvkeyonstandby 1
% /usr/bin/sudo /usr/bin/pmset -a hibernatemode 25
```

example:

```
% /usr/bin/sudo /usr/bin/pmset -a standbydelaylow 500
% /usr/bin/sudo /usr/bin/pmset -a standbydelayhigh 500
% /usr/bin/sudo /usr/bin/pmset -a highstandbythreshold 100
% /usr/bin/sudo /usr/bin/pmset -a destroyfvkeyonstandby 1
% /usr/bin/sudo /usr/bin/pmset -a hibernatemode 25
```

References:

1. https://www.lifewire.com/change-mac-sleep-settings-2260804
2. https://www.zdziarski.com/blog/?p=6705
3. https://www.howtogeek.com/260478/how-to-choose-when-your-mac-hibernates-or-enters-standby/

Additional Information:

The Ensure FileVault is Locked on Sleep recommendation has been removed. If your organization wants to continue setting FileVault lock, create or edit a configuration profile with the following information:

1. The `PayloadType` string is `com.apple.MCX`
2. The key to include is `DestroyFVKeyOnStandby`
3. The key must be set to

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

2.10.1.2 Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices (Automated)

Profile Applicability:

- Level 2

Description:

MacBooks should be set so that the sleep is 15 minutes or less and the display should sleep at 10 minutes or less. This setting should allow laptop users in most cases to stay within physically secured areas while going to a conference room, auditorium, or other internal location without having to unlock the encryption. When the user goes home at night, the laptop will auto-sleep after 15 minutes and to log back into the system when it resumes.

Note: If the screen saver is properly configured to the benchmark (15 minutes or less), then this recommendation will also pass no matter the `sleep` and `displaysleep` setting.

Rationale:

Laptops should sleep 15 minutes or less after sleeping.

Impact:

The laptop will take additional time to resume normal operation from sleep.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify sleep and hibernation settings:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPHardwareDataType | /usr/bin/grep
-e MacBook
```

If there is an output, verify if you are running an Apple processor:

```
% /usr/bin/sudo /usr/sbin/sysctl -n machdep.cpu.brand_string.
```

If output includes 'Apple', run the following:

```
% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep -e "^ sleep"
```

The output should be `sleep` with a value ≤ 15.

```
% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep -e "displaysleep"
```

The output should be `displaysleep` with a value ≤ 10 and ≤ the value of sleep.

example:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPHardwareDataType | grep -e
MacBook

      Model Name: MacBook Pro
      Model Identifier: MacBookPro18,3

% /usr/bin/sudo /usr/sbin/sysctl -n machdep.cpu.brand_string.
 Apple M1 Pro

% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep -e "^ sleep"

 sleep                15 (sleep prevented by sharingd, powerd, bluetoothd,
com.apple.PassKit.PaymentAuthor)

% /usr/bin/sudo /usr/bin/pmset -b -g | /usr/bin/grep -e "displaysleep"

 displaysleep         10
```

Note: If the screen saver is properly configured to the benchmark (15 minutes or less), then this recommendation will also pass no matter the `sleep` and `displaysleep` setting.

Internal Only - General

Remediation:

Terminal Method:

Run the following command to set the sleep time and hibernate mode:

```
% /usr/bin/sudo /usr/bin/pmset -a sleep <value≤15>
% /usr/bin/sudo /usr/bin/pmset -a displaysleep <value≤10 & < value of sleep>
```

example:

```
% /usr/bin/sudo /usr/bin/pmset -a sleep 15
% /usr/bin/sudo /usr/bin/pmset -a displaysleep 10
```

References:

1. https://www.lifewire.com/change-mac-sleep-settings-2260804
2. https://www.zdziarski.com/blog/?p=6705
3. https://www.howtogeek.com/260478/how-to-choose-when-your-mac-hibernates-or-enters-standby/

Additional Information:

The Ensure FileVault is Locked on Sleep recommendation has been removed. If your organization wants to continue setting FileVault lock, create or edit a configuration profile with the following information:

1. The `PayloadType` string is `com.apple.MCX`
2. The key to include is `DestroyFVKeyOnStandby`
3. The key must be set to

Hibernate mode has also been removed from this recommendation. Setting hibernate mode will require the user to log into the machine after sleep and disable any wake options. `hibernatemode` must be set to `25` or it will not force the computer into a pre-boot state. Organizations may still use this if there is a security need (ex. international travel), but it can cause kernel panics in Apple Silicon Macs. To enable hibernate mode, run the following command:

```
% /usr/bin/sudo /usr/bin/pmset -a hibernatemode 25
```


Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

2.10.2 Ensure Power Nap Is Disabled for Intel Macs (Automated)

Profile Applicability:

- Level 1

Description:

Power Nap allows the system to stay in low power mode, especially while on battery power, and periodically connect to previously known networks with stored credentials for user applications to phone home and get updates. This capability requires FileVault to remain unlocked and the use of previously joined networks to be risk accepted based on the SSID without user input.

This control has been updated to check the status on both battery and AC Power. The presence of an electrical outlet does not completely correlate with logical and physical security of the device or available networks.

Rationale:

Disabling this feature mitigates the risk of an attacker remotely waking the system and gaining access.

The use of Power Nap adds to the risk of compromised physical and logical security. The user should be able to decrypt FileVault and have the applications download what is required when the computer is actively used.

The control to prevent computer sleep has been retired for this version of the Benchmark. Forcing the computer to stay on and use energy in case a management push is needed is contrary to most current management processes. Only keep computers awake if after hours pushes are required on closed LANs.

Impact:

Power Nap exists for unattended user application updates like email and social media clients. With Power Nap disabled, the computer will not wake and reconnect to known wireless SSIDs intermittently when slept.

Internal Only - General

Audit:

Graphical Method:

Perform the following to verify that Power Nap is not enabled:

Desktop Instructions:

1. Open `System Settings`
2. Select `Energy Saver`
3. Verify that `Power Nap` is disabled
4. Select `UPS` (if applicable)
5. Verify that `Power Nap` is disabled

Laptop Instructions:

1. Open `System Settings`
2. Select `Battery`
3. Select `Power Adapter`
4. Verify that `Power Nap` is disabled
5. Select `Battery`
6. Verify that `Power Nap` is disabled
7. Select `UPS` (if applicable)
8. Verify that `Power Nap` is disabled

Note: To verify if you are running an Intel processor, perform the following steps:

1. Select in the `Menu Bar`
2. Select `About This Mac`
3. Verify that the `Chip` field included Intel

Terminal Method:

Run the following command to verify if Power Nap is disabled:

```
% /usr/bin/sudo /usr/bin/pmset -g custom | /usr/bin/grep -c "^\spowernap\s*1"

0
```

Note: To verify if you are running an Intel processor, run `/usr/sbin/sysctl -n machdep.cpu.brand_string`. The output will include `Intel`.

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to disable Power Nap:

Desktop Instructions:

1. Open `System Settings`
2. Select `Energy Saver`
3. Set `Power Nap` to disabled
4. Select `UPS` (if applicable)
5. Set `Power Nap` to disabled

Laptop Instructions:

1. Open `System Settings`
2. Select `Battery`
3. Select `Power Adapter` (for laptops only)
4. Set `Power Nap` to disabled
5. Select `Battery`
6. Set `Power Nap` to disabled
7. Select `UPS` (if applicable)
8. Set `Power Nap` to disabled

Terminal Method:

Run the following command to disable Power Nap:

```
% /usr/bin/sudo /usr/bin/pmset -a powernap 0
```


Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.10.3 Ensure Wake for Network Access Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

This feature allows the computer to take action when the user is not present and the computer is in energy saving mode. These tools require FileVault to remain unlocked and fully rejoin known networks. This macOS feature is meant to allow the computer to resume activity as needed regardless of physical security controls.

This feature allows other users to be able to access your computer’s shared resources, such as shared printers or Apple Music playlists, even when your computer is in sleep mode. In a closed network when only authorized devices could wake a computer, it could be valuable to wake computers in order to do management push activity. Where mobile workstations and agents exist, the device will more likely check in to receive updates when already awake. Mobile devices should not be listening for signals on any unmanaged network or where untrusted devices exist that could send wake signals.

Rationale:

Disabling this feature mitigates the risk of an attacker remotely waking the system and gaining access.

Impact:

Management programs like Apple Remote Desktop Administrator use wake-on-LAN to connect with computers. If turned off, such management programs will not be able to wake a computer over the LAN. If the wake-on-LAN feature is needed, do not turn off this feature.

The control to prevent computer sleep has been retired for this version of the Benchmark. Forcing the computer to stay on and use energy in case a management push is needed is contrary to most current management processes. Only keep computers awake if after hours pushes are required on closed LANs.

Turning off Wake for Network Access will also not allow Find My to work when the computer is asleep. It will also give this warning: "You won’t be able to locate, lock, or erase this Mac while it’s asleep because Wake for network access is turned off."

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify that Wake for network access is disabled:

Desktop Instructions:

1. Open `System Settings`
2. Select `Energy Saver`
3. Verify that `Wake for network access` is disabled

Laptop Instructions:

1. Open `System Settings`
2. Select `Battery`
3. Select `Options...`
4. Verify that `Wake for network access` is set to `Never`

Terminal Method:

Run the following command verify if Wake for network access is not enabled:

```
$ /usr/bin/sudo /usr/bin/pmset -g custom | /usr/bin/grep -e womp

womp                 0
```

or

Run the following command to verify that a profile is installed that disables Wake On Lan is installed:

```
% /usr/bin/sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "Wake On LAN"

                            "Wake On LAN" = 0;
                            "Wake On LAN" = 0;
                            "Wake On LAN" = 0;

% /usr/bin/sudo /usr/bin/profiles -P -o stdout | /usr/bin/grep "Wake On Modem
Ring"

                            "Wake On Modem Ring" = 0;
                            "Wake On Modem Ring" = 0;
                            "Wake On Modem Ring" = 0;
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to disable Wake for network access:

Desktop Instructions:

1. Open `System Settings`
2. Select `Energy Saver`
3. Set `Wake for network access` to disabled

Laptop Instructions:

1. Open `System Settings`
2. Select `Battery`
3. Select `Options...`
4. Set `Wake for network access` to `Never`

Terminal Method:

Run the following command to disable Wake for network access:

```
% /usr/bin/sudo /usr/bin/pmset -a womp 0
```


Internal Only - General

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.MCX`
2. The key to include is `com.apple.EnergySaver.desktop.ACPower`
3. The key must be set to:

```
<dict>
        <key>Wake On LAN</key>
        <integer>0</integer>
        <key>Wake On Modem Ring</key>
        <integer>0</integer>
</dict>
```

4. The key to also include is `com.apple.EnergySaver.portable.ACPower`
5. The key must be set to:

```
<dict>
        <key>Wake On LAN</key>
        <integer>0</integer>
        <key>Wake On Modem Ring</key>
        <integer>0</integer>
</dict>
```

6. The key to also include is `com.apple.EnergySaver.portable.BatteryPower`
7. The key must be set to:

```
<dict>
        <key>Wake On LAN</key>
        <integer>0</integer>
        <key>Wake On Modem Ring</key>
        <integer>0</integer>
</dict>
```

Note: Both `Wake on LAN` and `Wake on Modem Ring` need to be set. Only setting `Wake On LAN` will allow the profile to install but not set any settings. This profile will only apply the setting at installation and is not sticky.

Additional Information:

`/usr/bin/man pmset`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.11 Lock Screen

Internal Only - General

2.11.1 Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

A locking screen saver is one of the standard security controls to limit access to a computer and the current user's session when the computer is temporarily unused or unattended. In macOS, the screen saver starts after a value is selected in the drop-down menu. 15 minutes or less is an acceptable value. Any value can be selected through the command line or script, but a number that is not reflected in the GUI can be problematic. 15 minutes is the default for new accounts.

Rationale:

Setting an inactivity interval for the screen saver prevents unauthorized persons from viewing a system left unattended for an extensive period of time.

Impact:

If the screen saver is not set, users may leave the computer available for an unauthorized person to access information.

Audit:

Graphical Method:

Perform the following steps to verify that the screen saver is set to activate after less than or equal to 15 minutes of inactivity:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `Idle Time` set to `≤900`

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that enables a system-wide screensaver idle time of less than or equal to 15 minutes:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let timeout =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')
\
.objectForKey('idleTime'))
  if ( timeout <= 900 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Profile Method:

1. The PayloadType string is `com.apple.screensaver`
2. The key to include is `idleTime`
3. The key must be set to `<integer><≤900></integer>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

2.11.2 Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately (Automated)

Profile Applicability:

- Level 1

Description:

Sleep and screen saver modes are low power modes that reduce electrical consumption while the system is not in use.

Rationale:

Prompting for a password when waking from sleep or screen saver mode mitigates the threat of an unauthorized person gaining access to a system in the user's absence.

Impact:

Without a screenlock in place, anyone with physical access to the computer would be logged in and able to use the active user's session.

Audit:

Graphical Method:

Perform the following steps to verify that a password is required to wake from sleep or screen saver:

1. Open `System Settings`
2. Select `Lock Screen`
3. Verify that `Require password after screensaver begins or display is turned off` is set with `After 0 seconds` or `After 5 seconds`

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Ask For Password` set to `True`
5. Verify that the same installed profile has `Ask For Password Delay` set to `<0,5>`

Internal Only - General

Terminal Method:

Run the following command to verify that a password is required to wake the computer from sleep or from the screen saver after 5 seconds of less:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -screenLock status
```

The output should include either `screenLock delay is immediate` or `screenLock delay is 5 seconds`.

Run the following command to verify that a profile is installed that requires a password to wake the computer from sleep or from the screen saver:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')
\
  .objectForKey('askForPassword'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')
\
  .objectForKey('askForPasswordDelay'))
  if ( pref1 == 1 && pref2 <= 5 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to enable a password for unlock after a screen saver begins or after sleep:

1. Open `System Settings`
2. Select `Lock Screen`
3. Set `Require password after screensaver begins or display is turned off` to either `After 0 seconds` or `After 5 seconds`

Internal Only - General

Terminal Method:

Run the following command to require a password to unlock the computer after the screen saver engages or the computer sleeps:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -screenLock immediate -password
<administrator password>
```

or

```
% /usr/bin/sudo /usr/sbin/sysadminctl -screenLock 5 seconds -password
<administrator password>
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.screensaver`
2. The key to include is `askForPassword`
3. The key must be set to `<true/>`
4. The key to also include is `askForPasswordDelay`
5. The key must be set to `<integer><0,5></integer>`

References:

1. https://blog.kolide.com/screensaver-security-on-macos-10-13-is-broken-a385726e2ae2
2. https://github.com/rtrouton/profiles/blob/master/SetDefaultScreensaver/SetDefaultScreensaver.mobileconfig

Additional Information:

This only protects the system when the screen saver is running.

Note: The command line check in previous versions of the Benchmark does not work as expected here. The use of a profile is recommended for both implementation and auditing on a 10.13 system or later.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

Internal Only - General

2.11.3 Ensure a Custom Message for the Login Screen Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

An access warning informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored.

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Impact:

If users are not informed of their responsibilities, unapproved activities may occur. Users that are not approved for access may take the lack of a warning banner as implied consent to access.

Audit:

Graphical Method:

Perform the following steps to ensure that the a login banner is configured:

1. Open `System Settings`
2. Select `Lock Screen`
3. Verify `Show message when locked` is enabled
4. Select `Set`
5. Verify that the message displayed is configured to your organization's required text

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Banner Text` is configured to your organization's required text

Internal Only - General

Terminal Method:

Run the following command to verify that a custom message on the login screen is configured:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('LoginwindowText').js
EOS
```

The output should be a message that is configured to your organization's required text.

example:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('LoginwindowText').js
EOS

Center for Internet Security Test Message
```

Remediation:

Graphical Method:

Perform the following steps to enable a login banner set to your organization's required text:

1. Open `System Settings`
2. Select `Lock Screen`
3. Set `Show message when locked` to enabled
4. Select `Set`
5. Insert text in the `Set a message to appear on the lock screen` that matches your organization's required text
6. Select `Done`

Terminal Method:

Run the following command to enable a custom login screen message:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow LoginwindowText "<custom message>"
```

example:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow LoginwindowText "Center for
Internet Security Test Message"
```


Internal Only - General

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.loginwindow`
2. The key to include is `LoginwindowText`
3. The key must be set to `<string><Your organization's required text></string>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.11.4 Ensure Login Window Displays as Name and Password Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

The login window prompts a user for his/her credentials, verifies their authorization level, and then allows or denies the user access to the system.

Rationale:

Prompting the user to enter both their username and password makes it twice as hard for unauthorized users to gain access to the system since they must discover two attributes.

Audit:

Graphical Method:

Perform the following steps to verify that the login window displays name and password:

1. Open `System Settings`
2. Select `Lock Screen`
3. Verify that `Login window shows` is set to `Name and Password`

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Show Full Name` set to `True`

Terminal Method:

Run the following command to verify the login window displays name and password:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('SHOWFULLNAME').js
EOS

true
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to ensure the login window display name and password:

1. Open `System Settings`
2. Select `Lock Screen`
3. Set 'Login window shows' to `Name and Password`

Terminal Method:

Run the following command to enable the login window to display name and password:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow SHOWFULLNAME -bool true
```

Note: The GUI will not display the updated setting until the current user(s) logs out.

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.loginwindow`
2. The key to include is `SHOWFULLNAME`
3. The key must be set to `<true/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.11.5 Ensure Show Password Hints Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Password hints are user-created text displayed when an incorrect password is used for an account.

Rationale:

Password hints make it easier for unauthorized persons to gain access to systems by displaying information provided by the user to assist in remembering the password. This info could include the password itself or other information that might be readily discerned with basic knowledge of the end user.

Impact:

The user can set the hint to any value, including the password itself or clues that allow trivial social engineering attacks.

Audit:

Graphical Method:

Perform the following steps to verify if password hints are shown:

1. Open `System Settings`
2. Select `Lock Screen`
3. Verify that `Show password hints` is disabled

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Retires Before Hint Shown` set to `0`

Internal Only - General

Terminal Method:

Run the following command to verify that password hints are not displayed:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('RetriesUntilHint').js
EOS

0
```

Note: The default setting is not auditable through the command line. Please turn off the check and re-enable when the GUI does not reflect the audited results, or run the Terminal command(s).

Note: In macOS 26 Tahoe, setting the key `RetriesUntilHint` (or the plist) to a value other than `0` will result in the hint question mark icon appearing in the login window. Setting this to `0` is the only definitive way to ensure that does not appear.

Remediation:

Graphical Method:

Perform the following steps to disable password hints from being shown:

1. Open `System Settings`
2. Select `Lock Screen`
3. Set 'Show password hints` to disabled

Terminal Method:

Run the following command to disable password hints:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow RetriesUntilHint -int 0
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.loginwindow`
2. The key to include is `RetriesUntilHint`
3. The key must be set to `<integer>0</integer>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.12 Touch ID & Password (Login Password)

The `Touch ID & Password` `System Settings` pane is named `Login Password` on Macs that do not have Touch ID and does not contain any details about Touch ID.

Internal Only - General

2.12.1 Ensure Users' Accounts Do Not Have a Password Hint (Automated)

Profile Applicability:

- Level 1

Description:

Password hints help the user recall their passwords for various systems and/or accounts. In most cases, password hints are simple and closely related to the user's password.

Rationale:

Password hints that are closely related to the user's password are a security vulnerability, especially in the social media age. Unauthorized users are more likely to guess a user's password if there is a password hint. The password hint is very susceptible to social engineering attacks and information exposure on social media networks.

Audit:

Terminal Method:

Run the following command to verify that no users have a password hint:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint
```

The output will list all users. If there is any text listed with the user, then the machine is not compliant.

example:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -list /Users hint

firstuser    passwordhint
seconduser   passwordhint2
thirduser
fourthuser
Guest
```


Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to remove a user's password hint:

1. Open `System Settings`
2. Select `Touch ID & Passwords` (or `Login Password` on non-Touch ID Macs)
3. Select `Change...`
4. Change the password and ensure that no text is entered in the Password hint box

Note: This will only change the currently logged-in user's password, and not any others that are not compliant on the Mac. Use the terminal method if multiple users are not in compliance.

Terminal Method:

Run the following command to remove a user's password hint:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -delete /Users/<username>
hint
```

example:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -delete /Users/firstuser
hint

% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -delete /Users/seconduser
hint
```

Additional Information:

Organizations might consider entering an organizational help desk phone number or other text (such as a warning to the user). A help desk number is only appropriate for organizations with trained help desk personnel that are validating user identities for password resets.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

2.12.2 Audit Touch ID (Manual)

Profile Applicability:

- Level 1

Description:

Apple has integrated Touch ID with macOS and allows fingerprint use for many common operations. All use of Touch ID requires the presence of a password and the use of that password after every reboot, or when more than 48 hours has elapsed since the device was last unlocked. Touch ID is not a password replacement. The use of Touch ID can, however, make the use of passwords more secure for authorized users with physical access to a Mac. Normal day-to-day work operations can eliminate the use of console password entry unless a reboot is required other than on Monday morning. The infrequency of password screen unlock can enable a more complicated pass phrase that is seldom used. When Touch ID is used it remediates the risk of shoulder surfing (including video surveillance) to capture console credentials. There have been many reported shoulder surfing password captures on iOS devices. Reports have not been widespread on Macs, but shoulder surfing password capture is simpler than the other methods of breaking in to an encrypted Mac.

When a SmartCard or YubiKey is provisioned by an organization and is available for Console authentication, that is a much more secure option than the use of Touch ID and is preferred.

Rationale:

Touch ID allows for an account-enrolled fingerprint to access a key that uses a previously provided password.

Impact:

Touch ID is more convenient for use with aggressive screen lock controls.

Audit:

Graphical Method:

Perform the following to verify Touch ID settings:

1. Open `System Settings`
2. Select `Touch ID & Password`
3. Verify the Touch ID settings match your organization's requirements

Internal Only - General

Terminal Method:

For each user, run the following commands to verify that the Touch ID settings are within your organization's requirements:

```
% /usr/bin/sudo -u <username> /usr/bin/bioutil -r

User Touch ID configuration:
        Touch ID for unlock: <0,1>
        Touch ID for ApplePay: <0,1>
        Effective Touch ID for unlock: <0,1>
        Effective Touch ID for ApplePay: <0,1>

% /usr/bin/sudo /usr/bin/bioutil -r -s | /usr/bin/awk '/timeout/'

        Touch ID timeout (in seconds): <value≤172800>
```

Note: The `-s` notates a system configuration and does not need to be ran for each user.

Note: The output for unlock and ApplePay is `0` for disabled and `1` for enabled. The timeout value is seconds and can be set to any value.

example:

```
% /usr/bin/sudo -u firstuser /usr/bin/bioutil -r

User Touch ID configuration:
        Touch ID for unlock: 1
        Touch ID for ApplePay: 1
        Effective Touch ID for unlock: 1
        Effective Touch ID for ApplePay: 1

% /usr/bin/sudo usr/bin/bioutil -r -s | /usr/bin/awk '/timeout/'

        Touch ID timeout (in seconds): 172800
```

In the above example, the user has Touch ID enabled for both unlocking the system and for Apple Pay. The timeout for Touch ID is set to the maximum of 48 hours (172800 seconds).

Remediation:

Graphical Method:

Perform the following steps to set Touch ID to your organization's requirements:

1. Open `System Settings`
2. Select `Touch ID & Password`
3. Set the Touch ID settings to your organization's requirements

Internal Only - General

Terminal Method:

For each user, run the following commands to set Touch ID to your organization's requirements:

Use this command for Touch ID to unlock the system. Use `0` to disable unlock or `1` to enable unlock:

```
% /usr/bin/sudo -u <username> /usr/bin/bioutil -w -u <0,1>
```

Use this command for Touch ID to use Apple Pay. Use `0` to disable Apple Pay or `1` to enable Apple Pay:

```
% /usr/bin/sudo -u <username> /usr/bin/bioutil -w -a <0,1>
```

Use this command to set the timeout at the system level:

```
% /usr/bin/sudo usr/bin/bioutil -w -s -o <value≤172800>
```

example:

```
% /usr/bin/sudo -u <username> /usr/bin/bioutil -w -u 1

% /usr/bin/sudo -u <username> /usr/bin/bioutil -w -a 1

% /usr/bin/sudo usr/bin/bioutil -w -s -o 86400
```

Note: The `-s` notates a system configuration and does not need to be ran for each user.

References:

1. https://support.apple.com/guide/mac-help/touch-id-mchl16fbf90a/mac

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.13 Users & Groups

Account management is a central part of security for any computer system, including macOS. General practices should be followed to ensure that all accounts on a system are still needed, and that default accounts have been removed. Users with administrator roles should have distinct accounts for both administrator functions as well as day-to-day work where the passwords are different and known only by the user assigned to the account. Accounts with elevated privileges should not be easily discerned from the account name from standard accounts.

When any computer system is added to a directory system there are additional controls available, including user account management, that are not available in a standalone computer. One of the drawbacks is the local computer is no longer in control of the accounts that can access or manage it if given permission. For macOS, if the computer is connected to a directory, any standard user can now log into the computer at console, which by default may be desirable or not depending on the use case. If an administrator group is allowed to administer the local computer, the membership of that group is controlled completely in the directory.

macOS computers connected to a directory should be configured so that the risk is appropriate for the mission use of the computer. Only those accounts that require local authentication should be allowed, and only required administrator accounts should be in the local administrator group. Authenticated users for console access and domain admins for administration may be too broad or too limited.

Internal Only - General

2.13.1 Ensure Guest Account Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The guest account allows users access to the system without having to create an account or password. Guest users are unable to make setting changes and cannot remotely login to the system. All files, caches, and passwords created by the guest user are deleted upon logging out.

Rationale:

Disabling the guest account mitigates the risk of an untrusted user doing basic reconnaissance and possibly using privilege escalation attacks to take control of the system.

Impact:

A guest user can use that access to find out additional information about the system and might be able to use privilege escalation vulnerabilities to establish greater access.

Audit:

Graphical Method:

Perform the following steps to ensure that the guest account is not available:

1. Open `System Settings`
2. Select `Users & Groups`
3. Select the `i` next to the `Guest User`
4. Verify that `Allow guests to log in to this computer` is disabled

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Disable Guest Account` set to `True`
5. Verify that an installed profile has `Enable Guest Account` set to `False`

Internal Only - General

Terminal Method:

Run the following command to verify if the guest account is enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
  .objectForKey('DisableGuestAccount'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
  .objectForKey('EnableGuestAccount'))
  let pref3 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
\
  .objectForKey('GuestEnabled'))
  if (( pref1 == 1 && pref2 == 0 ) || ( pref3 == 0 )) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to disable guest account availability:

1. Open `System Settings`
2. Select `Users & Groups`
3. Select the `i` next to the `Guest User`
4. Set `Allow guests to log in to this computer` to disabled

Terminal Method:

Run the following command to disable the guest account:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow GuestEnabled -bool false
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.MCX`
2. The key to include is `DisableGuestAccount`
3. The key must be set to `<true/>`
4. The key to include is `EnableGuestAccount`
5. The key must be set to `<false/>`

Internal Only - General

Additional Information:

By default, the guest account is enabled for access to sharing services but is not allowed to log into the computer.

The guest account does not need a password when it is enabled to log into the computer.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

2.13.2 Ensure Guest Access to Shared Folders Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Allowing guests to connect to shared folders enables users to access selected shared folders and their contents from different computers on a network.

Rationale:

Not allowing guests to connect to shared folders mitigates the risk of an untrusted user doing basic reconnaissance and possibly using privilege escalation attacks to take control of the system.

Impact:

Unauthorized users could access shared files on the system.

Audit:

Graphical Method:

Perform the following steps to ensure that guests cannot connect to shared folders:

1. Open `System Settings`
2. Select `Users & Groups`
3. Select the `i` next to the `Guest User`
4. Verify that `Allow guests to connect to shared folders` is disabled

Terminal Method:

Run the following commands to verify that shared folders are not accessible to guest users:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -smbGuestAccess status
```

The output should include `SMB guest access disabled`.

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to no longer allow guest user access to shared folders:

1. Open `System Settings`
2. Select `Users & Groups`
3. Select the `i` next to the `Guest User`
4. Set `Allow guests to connect to shared folders` to disabled

Terminal Method:

Run the following commands to ensure that shared folders are not accessible to guest users:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -smbGuestAccess off
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Internal Only - General

2.13.3 Ensure Automatic Login Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The automatic login feature saves a user's system access credentials and bypasses the login screen. Instead, the system automatically loads to the user's desktop screen.

Rationale:

Disabling automatic login decreases the likelihood of an unauthorized person gaining access to a system.

Impact:

If automatic login is not disabled, an unauthorized user could gain access to the system without supplying any credentials.

Audit:

Graphical Method:

Perform the following steps to ensure that automatic login is not enabled:

1. Open `System Settings`
2. Select `Users & Groups`
3. Verify that `Automatic login in as...` is set to `Off`

or

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Disable Autologin` set to `True`

Internal Only - General

Terminal Method:

Run the following command to verify that automatic login has not been enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
\
  .objectForKey('com.apple.login.mcx.DisableAutoLoginClient'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
\
  .objectForKey('autoLoginUser'))
  if ( pref1 == 1 || pref2 == null ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Graphical Method:

Perform the following steps to set automatic login to off:

1. Open `System Settings`
2. Select `Users & Groups`
3. Set `Automatic login in as...` to `Off`

Terminal Method:

Run the following command to disable automatic login:

```
% /usr/bin/sudo /usr/bin/defaults delete
/Library/Preferences/com.apple.loginwindow autoLoginUser
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.loginwindow`
2. The key to include is `com.apple.login.mcx.DisableAutoLoginClient`
3. The key must be set to `<true/>`

Note: If both the profile is enabled and a user is set to autologin, the profile will take precedent. In this case, the graphical or terminal remediation method should also be applied in case the profile is ever removed.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

Internal Only - General

2.14 Game Center

Internal Only - General

2.14.1 Audit Game Center Settings (Manual)

Profile Applicability:

- Level 2

Description:

With macOS 10.13, Apple has introduced a separate section for Game Center in System Settings. It is possible to log in with the Apple ID and use the iCloud-based Game Center services.

Game Center is a feature from Apple that allows users to engage in game-related activities with friends when playing multiplayer games online on the Game Center social network. User profile data such as nickname, contact discovery, and also nearby players may be shared through iCloud.

Apple collects information here, such as the games users play and when they play them, all scores and achievements, and the challenges users send and receive. This information is used to track users' high scores, achievements, and challenges and to improve Game Center.

The automatic sign in to Game Center with AppleID should be disabled if not aligned with organizational rules

Personal profile visibility, Finding by Friends, requests from Contacts, Nearby Player detection and Connecting with Friends are all visibility options that should be risk accepted through an organizational policy before use.

Users should not sign in to Game Center on organizational managed devices if not covered under acceptable use. For personal devices Game Center should not be signed in if the user is not using Apple's gaming service.

Rationale:

Ensure Game Center service is used consistently with organizational requirements.

Impact:

Game Center is designed as a social network to use Apple's gaming service and includes capabilities to discover players in the service as through local network discovery. If the Apple feature is not needed it should not be on, and should not be signed in.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to verify the status of iCloud Game Center service:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `Allow GameCenter` set to your organization's requirements

Terminal Method:

Run the following command to verify that a profile is installed that sets iCloud allow GameCenter setting to your organization's requirements:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowGameCenter').js
EOS
```

If the output is `false`, Game Center is disabled. If the output is `true` Game Center is enabled.

Note: Since the profile method sets a system-wide setting, the individual user audit and/or remediation has been removed. We have included the individual user information in the additional information section for reference only.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `allowGameCenter`
3. The key should be set `<true/>`, to allow Game Center, or `<false/>`, to disable it, based on your organization's requirements

References:

1. https://support.apple.com/en-us/HT210401
2. https://developer.apple.com/documentation/devicemanagement/restrictions
3. https://developer.apple.com/game-center/
4. https://github.com/usnistgov/macos_security/pull/195

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

Internal Only - General

2.15 Notifications

Internal Only - General

2.15.1 Audit Notification Settings (Manual)

Profile Applicability:

- Level 1

Description:

Notification capabilities are designed to allow users to receive updates from applications that are not currently in use. These can be background applications or even notices from processes running on a computer that is not currently being actively used. Where the screen of a computer is visible to others other than the logged-in user due to shared working spaces or public spaces, consideration should be given to the exposure of sensitive data in notifications. Applications that use the system-wide application service may be individually managed, and applications that might expose confidential information to unauthorized users should not expose notifications except to the current user, especially on the locked screen when the computer may be unattended.

Rationale:

Some work environments will handle sensitive or confidential information with applications that can provide notifications to anyone who can see the computer screen. Organizations must review the likelihood that information may be exposed inappropriately and suppress notifications where risk is not organizationally accepted.

Impact:

Computer users are often juggling too much information through too many applications that want their attention and are often designed to get attention and never let it go. Notifications are a mechanism that can be used to cut through the deluge and allow important issues to be resolved in a timely way. Global controls on limiting user notifications, even for certain applications, could impact productivity and the timely remediation of issues.

Audit:

Graphical Method:

Perform the following steps to verify that Notifications are set to your organization's requirements:

1. Open `System Settings`
2. Select `Notifications`
3. Verify that `Show previews` for each application is set to your organization's requirements

Note: If the exposure of controlled information or data leakage is possible with application notifications, the acceptable notification level should be established through a risk analysis of what unauthorized leaks may occur.

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to set Notifications to your organization's requirements:

1. Open `System Settings`
2. Select `Notifications`
3. Select any applications that are not in compliance with your organization's requirements
4. Turn off or mute notifications that may expose information to unauthorized people that might be able to view screens of organizational computers.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.16 Wallet & Apple Pay

Internal Only - General

2.16.1 Audit Wallet & Apple Pay Settings (Manual)

Profile Applicability:

- Level 2

Description:

Touch ID is a prerequisite for using Apple Pay and Wallet on macOS. Apple Pay allows an Apple account holder to enroll their credit cards in Apple Pay and pay enrolled vendors without using the physical card or number. Apple's service eliminates the requirement to send the credit card number itself to the vendor. Apple Pay on a Mac allows the use of credit cards the user has already enrolled and reduces user risk for credit card purchases.

Rationale:

Some environments may have rules around purchases from organizationally managed computers and may want to discourage shopping from them. It is difficult to block access to websites that allow purchases, and Apple Pay has more controls for user protection than the manual entry of credit card information.

Audit:

Graphical Method:

Perform the following to verify Wallet & Apple Pay settings:

1. Open `System Settings`
2. Select `Wallet & Apple Pay`
3. Verify the `Wallet & Apple Pay` settings match your organization's requirements

Remediation:

Graphical Method:

Perform the following steps to set Wallet & Apple Pay to your organization's requirements:

1. Open `System Settings`
2. Select `Wallet & Apple Pay`
3. Set the `Wallet & Apple Pay` settings to your organization's requirements

References:

1. https://www.apple.com/apple-pay/
2. https://support.apple.com/guide/mac-help/use-wallet-apple-pay-on-mac-mchl4773988b/mac

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

Internal Only - General

2.17 Internet Accounts

Internet Accounts is an Apple feature to manage accounts for the use of Mac OS native applications. If Internet accounts are allowed and not tied to Enterprise SSO credentials, the use of the Internet Accounts setting allows for better tracking and control.

Disabling or hiding the System Preference Pane for Internet Accounts complicates the ability to audit and use OS level stored credentials. It does not block application access from a Mac to a domain that offers an authenticated session on the Internet.

Internal Only - General

2.17.1 Audit Internet Accounts for Authorized Use (Manual)

Profile Applicability:

- Level 1

Description:

Apple provides a section in System Settings to create and display Internet Accounts. Setting up an Internet Account allows the user to configure access to pre-existing accounts that are Internet Accessible. The Internet Accounts section is not managing network access to firewall rules, it only provides a location to manage credentials and audit external accounts for applications that make use of the "Internet Accounts." Some applications, like Thunderbird and Firefox, do not natively use Internet Accounts and store credentials with the application settings. Disabling the Internet Accounts section does not block access if network reachable, it just makes auditing and use more difficult. Depending on the maturity of network controls, auditing the providers listed in Internet Accounts is part of managing acceptable use.

Rationale:

Internet provided services may be restricted in your organization and should be reviewed. Even with an advanced application firewall, the user may not always be using an internal trusted network subject to the organizational firewall. An audit will document which services a user has configured.

Impact:

Risky services may be identified that are not authorized and will require a recess to work with the user to no longer connect from a managed Mac.

Audit:

Graphical Method:

Perform the following steps to verify what accounts have been added to Internet Accounts:

1. Open `System Settings`
2. Select `Internet Accounts`
3. Verify that all accounts are set to your organization's requirements

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to set accounts in Internet Accounts to your organization's requirements:

1. Open `System Settings`
2. Select `Internet Accounts`
3. For each account, select the account
4. Verify that each sync option is set to your organization's requirements
5. (Optional) Select `Delete Account...` to remove the account
6. (Optional) Select `Add Account...` to add an account to the system

References:

1. https://support.apple.com/guide/mac-help/add-your-email-and-other-accounts-mh35565/mac#:~:text=Add%20an%20account%20in%20Internet%20Accounts%20settings&text=On%20your%20Mac%2C%20choose%20Apple,may%20need%20to%20scroll%20down.)&text=Click%20Add%20Account%20on%20the,name%20of%20an%20account%20provider.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.18 Keyboard

Internal Only - General

2.18.1 Ensure On-Device Dictation Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

In macOS 14.0 Sonoma, Apple released the ability to limit dictation to staying on-device and not sending data to the Siri servers. The use of dictation is likely to include editing documents with confidential information. While Apple does have controls to obfuscate voice data that exists on their servers, it is recommended that Dictation-collected information does not leave the local Mac.

Rationale:

Sending data from dictation to the Siri servers could allow data spillage to occur. From a control perspective, it is much safer to ensure information of various levels of confidentiality is retained locally.

Impact:

Keeping all dictation on-device does not allow the system to better understand and learn, through machine learning, from the user.

Audit:

Terminal Method:

Run the following command to verify that a profile is installed to allow on-device dictation only:

```
% /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('forceOnDeviceOnlyDictation').js
EOS

true
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `forceOnDeviceOnlyDictation`
3. The key must be set to `<true/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

3 Logging and Auditing

This section provides guidance on configuring the logging and auditing facilities available in macOS. Starting with macOS 10.12, Apple introduced unified logging. This capability replaces the previous logging methodology with centralized, system-wide common controls. A full explanation of macOS logging behavior is beyond the scope of this Benchmark. These changes impact previous logging controls from macOS Benchmarks. At this point, many of the syslog controls have been or are being removed since the old logging methods have been deprecated. Controls that still appear useful will be retained. Some legacy controls have been removed for this release.

More info:

- https://developer.apple.com/documentation/os/logging
- https://eclecticlight.co/2018/03/19/macos-unified-log-1-why-what-and-how/

Internal Only - General

3.1 Ensure Security Auditing Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

macOS's audit facility, `auditd`, receives notifications from the kernel when certain system calls, such as `open`, `fork`, and `exit`, are made. These notifications are captured and written to an audit log.

Apple has deprecated `auditd` as of macOS 11.0 Big Sur. In macOS 14.0 Sonoma it is no longer enabled by default and it is suggested to use an application that integrates with the EndpointSecurity API. These applications are third party and not built into the macOS. Until `auditd` is removed from macOS completely, running the binary is the best way to collect logging in macOS and the only one that is part of the OS.

Rationale:

Logs generated by `auditd` may be useful when investigating a security incident as they may help reveal the vulnerable application and the actions taken by a malicious actor.

Audit:

Terminal Method:

Perform the following to verify that security auditing is enabled:

Run the following command to verify auditd:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -i auditd

-       0       com.apple.auditd
```

Remediation:

Terminal Method:

Perform the following to enable security auditing:

Run the following command to load auditd and create the `audit_control` file:

```
% /usr/bin/sudo /bin/launchctl load -w
/System/Library/LaunchDaemons/com.apple.auditd.plist

% /usr/bin/sudo /bin/cp /etc/security/audit_control.example
/etc/security/audit_control
```

References:

1. https://boberito.medium.com/auditd-the-logs-we-need-not-the-logs-we-deserve-cf1d8c83d15d

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

Internal Only - General

3.2 Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements (Automated)

Profile Applicability:

- Level 2

Description:

Auditing is the capture and maintenance of information about security-related events. Auditable events often depend on differing organizational requirements.

Rationale:

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises or attacks that have occurred, have begun, or are about to begin. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised.

Depending on the governing authority, organizations can have vastly different auditing requirements. In this control we have selected a minimal set of audit flags that should be a part of any organizational requirements. The flags selected below may not adequately meet organizational requirements for users of this benchmark. The auditing checks for the flags proposed here will not impact additional flags that are selected.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify the Security Auditing Flags that are enabled:

```
% /usr/bin/sudo /usr/bin/grep -e "^flags:" /etc/security/audit_control
```

The output should include the following flags:

- `aa` - audit all authorization and authentication events
- `ad` - audit all administrative events
- `-ex` - audit failed program execution
- `-fm` - audit failed file attribute modification events
- `-fr` - audit failed read actions where enforcement stops a read of a file
- `-fw` - audit failed write actions where enforcement stopped a file write
- `lo` - audit all login/logout events

The `-all` flag will capture all failed events across all audit classes and can be used to supersede the individual flags for failed events.

Note: Excluding potentially noisy audit events may be ideal, depending on your use-case.

Note: Historical audit flags are listed below as preliminary guidance.

Remediation:

Terminal Method:

Perform the following to set the required Security Auditing Flags:

Edit the `/etc/security/audit_control` file and add `aa`, `ad`, `-ex`, `-fm`, `-fr`, `-fw`, and `lo` to `flags`. You can also substitute `-all` for `-ex`, `-fm`, `-fr`, and `-fw`.

References:

1. https://derflounder.wordpress.com/2012/01/30/openbsm-auditing-on-mac-os-x/
2. https://www.scip.ch/en/?labs.20150108
3. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
4. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf
5. https://github.com/usnistgov/macos_security

Additional Information:

Flag settings are currently based on the guidance provided by the NIST through the macOS Security guidance they are providing in their GitHub repository. You can find that guidance here.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

Internal Only - General

3.3 Ensure install.log Is Retained for 365 or More Days and No Maximum Size (Automated)

Profile Applicability:

- Level 1

Description:

macOS writes information pertaining to system-related events to the file `/var/log/install.log` and has a configurable retention policy for this file. The default logging setting limits the file size of the logs and the maximum size for all logs. The default allows for an errant application to fill the log files and does not enforce sufficient log retention. The Benchmark recommends a value based on standard use cases. The value should align with local requirements within the organization.

The default value has an "all_max" file limitation, no reference to a minimum retention, and a less precise rotation argument.

The all_max flag control will remove old log entries based only on the size of the log files. Log size can vary widely depending on how verbose installing applications are in their log entries. The decision here is to ensure that logs go back a year, and depending on the applications a size restriction could compromise the ability to store a full year.

While this Benchmark is not scoring for a rotation flag, the default rotation is sequential rather than using a timestamp. Auditors may prefer timestamps in order to simply review specific dates where event information is desired.

Please review the File Rotation section in the man page for more information.

```
man asl.conf
```

- The maximum file size limitation string should be removed "all_max="
- An organization-appropriate retention should be added "ttl="
- The rotation should be set with timestamps "rotate=utc" or "rotate=local"

Rationale:

Archiving and retaining `install.log` for at least a year is beneficial in the event of an incident as it will allow the user to view the various changes to the system along with the date and time they occurred.

Impact:

Without log files system maintenance and security, forensics cannot be properly performed.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify that log files are retained for at least 365 days with no maximum size:

```
% /usr/bin/sudo /usr/bin/grep -i ttl /etc/asl/com.apple.install
```

The output must include `ttl≥365`

```
% /usr/bin/sudo /usr/bin/grep -i all_max= /etc/asl/com.apple.install
```

No results should be returned.

Remediation:

Terminal Method:

Perform the following to ensure that install logs are retained for at least 365 days:

Edit the `/etc/asl/com.apple.install` file and add or modify the `ttl` value to `365` or greater on the `file` line. Also, remove the `all_max=` setting and value from the `file` line.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●
v7	6.7 Regularly Review Logs On a regular basis, review logs to identify anomalies or abnormal events.		●	●

Internal Only - General

3.4 Ensure Security Auditing Retention Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

The macOS audit capability contains important information to investigate security or operational issues. This resource is only completely useful if it is retained long enough to allow technical staff to find the root cause of anomalies in the records.

Retention can be set to respect both size and longevity. To retain as much as possible under a certain size, the recommendation is to use the following:

`expire-after:60d OR 5G`

This recommendation is based on minimum storage for review and investigation. When a third party tool is in use to allow remote logging or the store and forwarding of logs, this local storage requirement is not required.

Rationale:

The audit records need to be retained long enough to be reviewed as necessary.

Impact:

The recommendation is that at least 60 days or 5 gigabytes of audit records are retained. Systems that have very little remaining disk space may have issues retaining sufficient data.

Audit:

Terminal Method:

Run the following command to verify audit retention:

```
% /usr/bin/sudo /usr/bin/grep -e "^expire-after" /etc/security/audit_control
```

The output value for `expire-after:` should be ≥ `60d OR 5G`

Note: If your organization is offloading your security logs, we recommend following the same guidance (at minimum) for your off-site log storage. Your local storage limit (or time frame) may fail if they are set to lower in this case, but are following the guidance.

Remediation:

Terminal Method:

Perform the following to set the audit retention length:

Edit the `/etc/security/audit_control` file so that `expire-after:` is at least `60d OR 5G`

Internal Only - General

Default Value:

More info in the man page. To reference the man page use the command `$ man audit_control`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●
v7	6.7 Regularly Review Logs On a regular basis, review logs to identify anomalies or abnormal events.		●	●

Internal Only - General

3.5 Ensure Access to Audit Records Is Controlled (Automated)

Profile Applicability:

- Level 1

Description:

The audit system on macOS writes important operational and security information that can be both useful for an attacker and a place for an attacker to attempt to obfuscate unwanted changes that were recorded. As part of defense-in-depth, the `/etc/security/audit_control` configuration and the files in `/var/audit` should be owned only by root with group wheel with read-only rights and no other access allowed. macOS ACLs should not be used for these files.

The default folder for storing logs is `/var/audit`, but it can be changed. This recommendation will ensure that any target directory has appropriate access control in place even if the target directory is not the default of `/var/audit`.

Rationale:

Audit records should never be changed except by the system daemon posting events. Records may be viewed or extracts manipulated, but the authoritative files should be protected from unauthorized changes.

Impact:

This control is only checking the default configuration to ensure that unwanted access to audit records is not available.

Internal Only - General

Audit:

Terminal Method:

Run the following commands to check file access rights:

```
% /usr/bin/sudo /bin/ls -n /etc/security/audit_control | /usr/bin/awk
'{s+=$3} END {print s}'

0

% /usr/bin/sudo /bin/ls -n /etc/security/audit_control | /usr/bin/awk
'{s+=$4} END {print s}'

0

% /usr/bin/sudo /bin/ls -n /etc/security/audit_control | /usr/bin/awk '!/-r--
r-----|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '

0

% /usr/bin/sudo /bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control
| /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$3} END {print s}'

0

$ /usr/bin/sudo /bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control
| /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$4} END {print s}'

0

$ /usr/bin/sudo /bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control
| /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '!/-r--r-----
|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '

0
```


Internal Only - General

Remediation:

Terminal Method:

Run the following to commands to set the audit records to the root user and wheel group:

```
% /usr/bin/sudo /usr/sbin/chown -R root:wheel /etc/security/audit_control

% /usr/bin/sudo /bin/chmod -R 440 /etc/security/audit_control

% /usr/bin/sudo /usr/sbin/chown -R root:wheel $(/usr/bin/sudo /usr/bin/grep
'^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')

% /usr/bin/sudo /bin/chmod -R 440 $(/usr/bin/grep '^dir'
/etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

Note: It is recommended to do a thorough verification process on why the audit logs have been changed before following the remediation steps. If the system has different access controls on the audit logs, and the changes cannot be traced, a new install may be prudent. Check for signs of file tampering as well as unapproved OS changes.

Note: In macOS 14, and versions going forward, Apple disabled `auditd` by default. Since that is the default, the `/etc/security/audit_control` does not exist. If this remediation is ran without copying the `/etc/security/audit_control.example` to `/etc/security/audit_control` then it can cause a recursive permissions issue and can cause an unsupported state (undesired results) and booting anomalies.

Additional Information:

From `ls` man page

```
-e      Print the Access Control List (ACL) associated with the file, if
             present, in long (-l) output.
```

More info:

https://www.techrepublic.com/blog/apple-in-the-enterprise/introduction-to-os-x-access-control-lists-acls/

http://ahaack.net/technology/OS-X-Access-Control-Lists-ACL.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Internal Only - General

3.6 Audit Software Inventory (Manual)

Profile Applicability:

- Level 2

Description:

With the introduction of Mac OS X 10.6.6, Apple added a new application, App Store, which resides in the Applications directory. This application allows a user with admin privileges and an Apple Account to browse Apple's online App Store, purchase (including no-cost purchases), and install new applications, bypassing Enterprise software inventory controls. Any admin user can install software in the /Applications directory whether from internet downloads, thumb drives, optical media, cloud storage, or even binaries through email. Even standard users can run executables downloaded to their home folder by default. The source of the software is not nearly as important as a consistent audit of all installed software for patch compliance and appropriateness.

A single user desktop where the user, administrator, and the person approving software are all the same person probably does not need to audit software inventory to this extent. It is helpful in the case of stability problems or malware, however.

Scan systems on a monthly basis and determine the number of unauthorized pieces of software that are installed. Verify that if an unauthorized piece of software is found one month, it is removed from the system the next.

Export System Information through the built-in System Information Application or other third-party tools on an organizationally defined timetable.

Rationale:

Part of comprehensive IT security involves device management and ensuring that all software is authorized and patched. Checking for macOS updates and app updates are relatively simple for the end user, and can even be updated with minimal privileges from trusted sources, if enabled. Remote monitoring of the patch status for software maintained through Apple is very well supported by management applications. Neither Apple capabilities nor third-party patch management solutions will cover all mission-necessary software for most organizations. Full visibility into software present on the system enables vulnerability and risk management.

P.S. Don't forget about browser plugins/extensions for all installed software.

Internal Only - General

Audit:

Graphical Mode:

Perform the following steps to access System Information:

1. Open `/Applications/Utilities/System Information`
2. Select `Software`
3. Select `System Report`
4. Select `Applications`
5. Verify that no Applications listed are against your organization's requirements
6. Select `Installations`
7. Verify that no Installations listed are against your organization's requirements

Terminal Method:

Run the following command to view all System Profiler details

```
% /usr/bin/sudo /usr/sbin/system_profiler SPApplicationsDataType
```

Remediation:

Delete any unnecessary applications from the system.

References:

1. https://support.apple.com/en-us/HT203001
2. https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.1 Establish and Maintain a Software Inventory Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	●	●	●
v7	2.1 Maintain Inventory of Authorized Software Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	●	●	●

Internal Only - General

4 Network Configurations

This section contains guidance on configuring the networking-related aspects of macOS that have been removed from `System Settings` but still can be set through `Terminal`.

Internal Only - General

4.1 Ensure Bonjour Advertising Services Is Disabled (Automated)

Profile Applicability:

- Level 2

Description:

Bonjour is an auto-discovery mechanism for TCP/IP devices which enumerates devices and services within a local subnet. DNS on macOS is integrated with Bonjour and should not be turned off, but the Bonjour advertising service can be disabled.

Rationale:

Bonjour can simplify device discovery from an internal rogue or compromised host. An attacker could use Bonjour's multicast DNS feature to discover a vulnerable or poorly-configured service or additional information to aid a targeted attack. Implementing this control disables the continuous broadcasting of "I'm here!" messages. Typical end-user endpoints should not have to advertise services to other computers. This setting does not stop the computer from sending out service discovery messages when looking for services on an internal subnet, if the computer is looking for a printer or server and using service discovery. To block all Bonjour traffic except to approved devices, the pf or other firewall would be needed.

Impact:

Some applications may not operate properly if Bonjour advertising (discoverable) is turned off. In AirDrop, having this discoverability feature disabled makes the system unavailable to receive files in AirDrop on the local network.

Audit:

Graphical Method:

Perform the following steps to ensure that Bonjour Advertising is disabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `NoMulticastAdvertisements` set to `1`

Internal Only - General

Terminal Method:

Run the following command to verify that Bonjour Advertising is not enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mDNSResponder')\
.objectForKey('NoMulticastAdvertisements').js
EOS

true
```

Remediation:

Terminal Method:

Run the following command to disable Bonjour Advertising services:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.mDNSResponder.plist NoMulticastAdvertisements
-bool true
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mDNSResponder`
2. The key to include is `NoMulticastAdvertisements`

Additional Information:

Anything Bonjour discovers is already available on the network and probably discoverable with network scanning tools. The security benefit of disabling Bonjour for that reason is minimal.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

4.2 Ensure HTTP Server Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

macOS used to have a graphical front-end to the embedded Apache web server in the operating system. Personal web sharing could be enabled to allow someone on another computer to download files or information from the user's computer. Personal web sharing from a user endpoint has long been considered questionable, and Apple has removed that capability from the GUI. Apache, however, is still part of the Operating System and can be easily turned on to share files and provide remote connectivity to an end-user computer. Web sharing should only be done through hardened web servers and appropriate cloud services.

Rationale:

Web serving should not be done from a user desktop. Dedicated web servers or appropriate cloud storage should be used. Open ports make it easier to exploit the computer.

Impact:

The web server is both a point of attack for the system and a means for unauthorized file transfers.

Audit:

Terminal Method:

Run the following command to verify that the HTTP server services are not currently enabled. This check does not reflect any auto-start settings, only whether the web server is currently enabled:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -c "org.apache.httpd"

0
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to disable the HTTP server services:

```
% /usr/bin/sudo /usr/sbin/apachectl stop

% /usr/bin/sudo /bin/launchctl unload -w
/System/Library/LaunchDaemons/org.apache.httpd.plist
```

References:

1. https://www.stigviewer.com/stig/apple_macos_11_big_sur/2021-06-16/finding/V-230793
2. https://httpd.apache.org/security/vulnerabilities_24.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

4.3 Ensure NFS Server Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

macOS can act as an NFS fileserver. NFS sharing could be enabled to allow someone on another computer to mount shares and gain access to information from the user's computer. File sharing from a user endpoint has long been considered questionable, and Apple has removed that capability from the GUI. NFSD is still part of the Operating System and can be easily turned on to export shares and provide remote connectivity to an end-user computer.

The etc/exports file contains the list of NFS shared directories. If the file exists, it is likely that NFS sharing has been enabled in the past or may be available periodically. As an additional check, the audit verifies that there is no /etc/exports file.

Rationale:

File serving should not be done from a user desktop. Dedicated servers should be used. Open ports make it easier to exploit the computer.

Impact:

The nfs server is both a point of attack for the system and a means for unauthorized file transfers.

Audit:

Terminal Method:

Run the following commands to verify that the NFS fileserver service is not enabled:

```
% /usr/bin/sudo /sbin/nfsd status | /usr/bin/awk '/nfsd service/ { print
$NF}'

disabled

% /usr/bin/sudo /bin/cat /etc/exports

cat: /etc/exports: No such file or directory
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to disable the nfsd fileserver services:

```
% /usr/bin/sudo /bin/launchctl disable system/com.apple.nfsd
```

Remove the exported Directory listing.

```
% /usr/bin/sudo /bin/rm -rf /etc/exports
```

Note: Removing `/etc/exports` also stops the `NFS` service if it was running.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

5 System Access, Authentication and Authorization

The controls in this section are a combination of hardening controls that are not specifically in a System Settings pane. Many of these controls are only accessible using the Command Line or a Device Profile and not available in the Graphical User Interface. The Benchmark does contain simple, easy to follow instructions for technical staff to audit and implement recommended controls.

Internal Only - General

5.1 File System Permissions and Access Controls

File system permissions have always been part of computer security. There are several principles that are part of best practices for a POSIX-based system which are contained in this section. This section does not contain a complete list of every permission on a macOS System that might be problematic. Developers and use cases differ, and what some administrators who are long in the profession might consider a travesty are issues to which a risk assessor steeped in BYOD trends may not give a second glance. Here we document controls that should point out truly bad practices or anomalies which should be looked at and considered closely. Many of the controls are to mitigate the risk of privilege escalation attacks and data exposure to unauthorized parties.

Internal Only - General

5.1.1 Ensure Home Folders Are Secure (Automated)

Profile Applicability:

- Level 1

Description:

By default, macOS allows all valid users into the top level of every other user's home folder and restricts access to the Apple default folders within. Another user on the same system can see you have a "Documents" folder but cannot see inside it. This configuration does work for personal file sharing but can expose user files to standard accounts on the system.

The best parallel for Enterprise environments is that everyone who has a Dropbox account can see everything that is at the top level but can't see your pictures. Similarly with macOS, users can see into every new Directory that is created because of the default permissions.

Home folders should be restricted to access only by the user. Sharing should be used on dedicated servers or cloud instances that are managing access controls. Some environments may encounter problems if execute rights are removed as well as read and write. Either no access or execute only for group or others is acceptable.

Rationale:

Allowing all users to view the top level of all networked users' home folder may not be desirable since it may lead to the revelation of sensitive information.

Impact:

If implemented, users will not be able to use the "Public" folders in other users' home folders. "Public" folders with appropriate permissions would need to be set up in the /Shared folder.

Internal Only - General

Audit:

Terminal Method:

Run the following command to ensure that all home folders are secure:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -
maxdepth 1 -type d -not -perm 700 | /usr/bin/grep -v "Shared" | /usr/bin/grep
-v "Guest"
```

The output will show what user folders are not secure.

example:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -
maxdepth 1 -type d -not -perm 700 -not -perm 710 -not -perm 711 |
/usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest"

/System/Volumes/Data/Users/firstuser
/System/Volumes/Data/Users/thirduser
```

Alternately, run the following command if there needs to be executable access for a home folder:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -
maxdepth 1 -type d -not -perm 700 -not -perm 710 -not -perm 711 |
/usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest"
```

The output will show what user folders are not secure.

example:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -
maxdepth 1 -type d -not -perm 700 -not -perm 710 -not -perm 711 |
/usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest"

/System/Volumes/Data/Users/firstuser
/System/Volumes/Data/Users/thirduser
```


Internal Only - General

Remediation:

Terminal Method:

For each user, run the following command to secure all home folders:

```
% /usr/bin/sudo /bin/chmod -R og-rwx /Users/<username>
```

Alternately, run the following command if there needs to be executable access for a home folder:

```
% /usr/bin/sudo /bin/chmod -R og-rw /Users/<username>
```

example:

```
% /usr/bin/sudo /bin/chmod -R og-rw /Users/firstuser/

% /usr/bin/sudo /bin/chmod -R og-rwx /Users/thirduser/
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Internal Only - General

5.1.2 Ensure System Integrity Protection Status (SIP) Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

System Integrity Protection is a security feature introduced in OS X 10.11 El Capitan. System Integrity Protection restricts access to System domain locations and restricts runtime attachment to system processes. Any attempt to inspect or attach to a system process will fail. Kernel Extensions are now restricted to /Library/Extensions and are required to be signed with a Developer ID.

Rationale:

Running without System Integrity Protection on a production system runs the risk of the modification of system binaries or code injection of system processes that would otherwise be protected by SIP.

Impact:

System binaries and processes could become compromised.

Audit:

Terminal Method:

Run the following command to verify that System Integrity Protection is enabled:

```
% /usr/bin/sudo /usr/bin/csrutil status

`System Integrity Protection status: enabled.`
```


Internal Only - General

Remediation:

Terminal Method:

Perform the following steps to enable System Integrity Protection:

1. Reboot into the `Recovery Partition` (reboot and hold down `Command (⌘)` + `R`)
2. Select `Utilities`
3. Select `Terminal`
4. Run the following command:

```
# /usr/bin/sudo /usr/bin/csrutil enable

Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.
```

5. Reboot the computer

Note: You should research why the system had SIP disabled. It might be a better option to erase the Mac and reinstall the operating system. That is at your discretion.

Note: You cannot enable System Integrity Protection from the booted operating system. If the remediation is attempted in the booted OS and not the Recovery Partition the output will give the error `csrutil: failed to modify system integrity configuration. This tool needs to be executed from the Recovery OS.`

References:

1. https://developer.apple.com/documentation/security/disabling_and_enabling_system_integrity_protection
2. https://support.apple.com/en-us/HT204899

Additional Information:

Related to SIP controls, Library Validation is a security feature introduced in macOS 10.10 Yosemite. Library Validation protects processes from loading arbitrary libraries. This stops root from loading arbitrary libraries into any process (depending on SIP status), and keeps root from becoming more powerful. Security is strengthened, because some user processes can no longer be fooled to run additional code without root's explicit request, which may grant access to daemons that depend on Library Validation for secure validation of code identity.

With SIP enabled, Library Validation cannot be disabled. To test against a non-validated library, you will need to disabled SIP AND disable Library Validation.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

Internal Only - General

5.1.3 Ensure Apple Mobile File Integrity (AMFI) Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple Mobile File Integrity (AMFI) was first released in macOS 10.12. The daemon and service block attempts to run unsigned code. AMFI uses launchd, code signatures, certificates, entitlements, and provisioning profiles to create a filtered entitlement dictionary for an app. AMFI is the macOS kernel module that enforces code-signing and library validation.

Rationale:

Apple Mobile File Integrity validates that application code is validated.

Impact:

Applications could be compromised with malicious code.

Audit:

Terminal Method:

Run the following command to verify that Apple Mobile File Integrity is enabled:

```
% /usr/bin/sudo /usr/sbin/nvram -p | /usr/bin/grep -c
"amfi_get_out_of_my_way=1"

0
```

Note: AMFI cannot be disabled with SIP enabled, but a change attempt can be made that will appear successful, and report incorrectly as successful. If the AMFI audit fails, and the SIP audit passes, this is still an issue the admin should research.

Remediation:

Terminal Method:

Run the following command to enable the Apple Mobile File Integrity service:

```
% /usr/bin/sudo /usr/sbin/nvram boot-args=""
```

References:

1. https://eclecticlight.co/2018/12/29/amfi-checking-file-integrity-on-your-mac/
2. https://github.com/usnistgov/macos_security/issues/39
3. https://github.com/usnistgov/macos_security/issues/40
4. https://www.naut.ca/blog/2020/11/13/forbidden-commands-to-liberate-macos/

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

Internal Only - General

5.1.4 Ensure Signed System Volume (SSV) Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Signed System Volume is a security feature introduced in macOS 11.0 Big Sur.

During system installation, a SHA-256 cryptographic hash is calculated for all immutable system files and stored in a Merkle tree which itself is hashed as the Seal. Both are stored in the metadata of the snapshot created of the System volume.

The seal is verified by the boot loader at startup. macOS will not boot if system files have been tampered with. If validation fails, the user will be instructed to reinstall the operating system.

During read operations for files located in the Signed System Volume, a hash is calculated and compared to the value stored in the Merkle tree.

Rationale:

Running without Signed System Volume on a production system could run the risk of Apple software that integrates directly with macOS being modified.

Impact:

Apple Software that integrates with the operating system could become compromised.

Audit:

Terminal Method:

Run the following command to verify that Signed System Volume is enabled:

```
% /usr/bin/sudo /usr/bin/csrutil authenticated-root status

Authenticated Root status: enabled
```

Remediation:

If SSV has been disabled, assume that the operating system has been compromised. Back up any files, and do a clean install to a known good Operating System.

Internal Only - General

References:

1. https://developer.apple.com/news/?id=3xpv8r2m
2. https://eclecticlight.co/2020/11/30/is-big-surs-system-volume-sealed/
3. https://eclecticlight.co/2020/06/25/big-surs-signed-system-volume-added-security-protection/
4. https://support.apple.com/guide/security/signed-system-volume-security-secd698747c9/web
5. https://support.apple.com/guide/mac-help/what-is-a-signed-system-volume-mchl0f9af76f/mac

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

Internal Only - General

5.1.5 Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated)

Profile Applicability:

- Level 1

Description:

Applications in the System Applications Directory (/Applications) should be world-executable since that is their reason to be on the system. They should not be world-writable and allow any process or user to alter them for other processes or users to then execute modified versions.

Rationale:

Unauthorized modifications of applications could lead to the execution of malicious code.

Impact:

Applications changed will no longer be world-writable. Depending on the environment, there will be different risk tolerances on each non-conforming application. Global changes should not be performed where mission-critical applications are misconfigured.

Audit:

Terminal Method:

Run the following command to verify that all applications have the correct permissions:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Applications -iname
"*\.app" -type d -perm -2 -ls | grep -v Xcode.app | /usr/bin/wc -l |
/usr/bin/xargs

0
```

Remediation:

Terminal Method:

Run the following command to change the permissions for each application that does not meet the requirements:

```
% /usr/bin/sudo IFS=$'\n'
for apps in $( /usr/bin/find /System/Volumes/Data/Applications -iname
"*\.app" -type d -perm -2 | grep -v Xcode.app ); do
  /bin/chmod -R o-w "$apps"
done
```

Note: Global changes should not be performed where mission-critical applications are part of the improperly permissioned applications.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Internal Only - General

5.1.6 Ensure No World Writable Folders Exist in the System Folder (Automated)

Profile Applicability:

- Level 1

Description:

Software sometimes insists on being installed in the `/System/Volumes/Data/System` Directory and has inappropriate world-writable permissions.

Macs with writable files in System should be investigated forensically. A file with open writable permissions is a sign of at best a rogue application. It could also be a sign of a computer compromise and a persistent presence on the system.

Rationale:

Folders in `/System/Volumes/Data/System` should not be world-writable. The audit check excludes the `downloadDir` and `locks` folders that are part of Apple's default user template.

Impact:

Changing file permissions could disrupt the use of applications that rely on files in the System Folder with vulnerable permissions.

Audit:

Terminal Method:

Run the following command to check for directories in the /System folder that are world-writable:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/System -type d -perm -2 -
ls | /usr/bin/grep -vE "downloadDir|locks" | /usr/bin/wc -l | /usr/bin/xargs

0
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to set permissions so that folders are not world-writable in the /System folder:

```
% /usr/bin/sudo IFS=$'\n'
  for sysPermissions in $( /usr/bin/find /System/Volumes/Data/System -type d
-perm -2 | /usr/bin/grep -vE "downloadDir|locks" ); do
    /bin/chmod -R o-w "$sysPermissions"
  done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Internal Only - General

5.1.7 Ensure No World Writable Folders Exist in the Library Folder (Automated)

Profile Applicability:

- Level 2

Description:

Software sometimes insists on being installed in the `/System/Volumes/Data/Library` directory and has inappropriate world-writable permissions. This software could be compromised with the folder(s) being world-writable by unauthorized actions.

Rationale:

Folders in `/System/Volumes/Data/Library` should not be world-writable. The audit check excludes folders where the sticky bit is set by Apple. These folders are required by the operating system to run and should not be modified.

Some security vendors use a world-writable folder for their security extension tool. This will be considered compliant due to the tools themselves not allowing a user to write to their folders. This is against the standard practice on POSIX systems. It is considered compliant here because of additional security vendor controls that are controlled through industry standard mitigations.

Impact:

Applications that are not following standard practices, and have world-writable files in `/System/Volumes/Data/Library` may not launch or operate correctly after the remediation has been run. The vendor(s) of the software(s) should be notified so they can update their software(s) to follow standard practices. Organizations will have to make risk decisions on the continued operation of this software.

Audit:

Terminal Method:

Run the following to verify that no directories in the `/System/Volumes/Data/Library` folder are world-writable:

```
% /usr/bin/sudo
/usr/bin/find /Library -type d -perm -002 ! -perm -1000 ! -xattrname
com.apple.rootless 2>/dev/null | /usr/bin/wc -l | /usr/bin/xargs

0
```

Note: To see what folders have world-writable permissions, run the command `/usr/bin/find /Library -type d -perm -002 ! -perm -1000 ! -xattrname com.apple.rootless 2>/dev/null`

Internal Only - General

Remediation:

Terminal Method:

Run the following command to set permissions so that folders are not world-writable in the `/System/Volumes/Data/Library` folder:

```
% /usr/bin/sudo IFS=$'\n'
for libPermissions in $(/usr/bin/find /Library -type d -perm -002 ! -perm -
1000 ! -xattrname com.apple.rootless 2>/dev/null); do
  /bin/chmod -R o-w "$libPermissions"
done
```

References:

1. https://attack.mitre.org/techniques/T1222/002/
2. https://attack.mitre.org/mitigations/M1022/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Internal Only - General

5.2 Account and Password Policy Management

Password security is an important part of general IT security where passwords are in use. For macOS, passwords are still much more widely used than other methods for account access. While there are other authentication and authorization methods for access from a macOS computer to organizational services, console access to the Mac is probably done using a password. This section contains password controls.

Apple has provided sufficient security controls to resist password attacks against the locked console, thus the CIS benchmark no longer recommends locking the keychain in addition to locking the console or display.

Recent updates based on research by NIST in SP800-63 call into question traditional password complexity and rotation requirements. Sticky notes are not a password management program, and password vault APIs are under increasing attack. Ideally, the user will remember their important passwords. The new understanding has informed changes to the previous password recommendations.

Length, threshold, and a yearly rotation requirement are the only scored controls below. Other controls will remain as unscored options. Passwords used for macOS are likely to also function as encryption keys for FileVault. Depending on the information confidentiality on FileVault volumes, stronger passwords may be required than are necessary to pass the controls in this Benchmark.

Apple-supported solutions for managing local passwords on macOS are to use either an XML file that contains password rules that are imported with `pwpolicy` or through the use of a profile. In either case, the controls in this section can be implemented with an organizationally-approved password policy.

A better solution to macOS security is to reduce the use of passwords by using the included smart card capabilities from Apple. This capability can be used with both a traditional PIV or CAC card but also with Yubikeys. Where possible replace passwords in your organization with included cryptographically secure technologies. Apple - Use a smart card on Mac Support Documentation and YubiKey support - YubiKey for macOS login

Before applying your organization's password policy, the existing password policy should be cleared so there is no outdated or conflicting legacy settings in the password policy. A pre-existing password policly could result in false results. To clear the password policy before applying the newest options, use the command `/usr/bin/sudo /usr/bin/pwpolicy -clearaccountpolicies`.

After policies are set, to force a user to change their password on their next login, use the command `/usr/bin/pwpolicy -u <username> -setpolicy "newPasswordRequired=1"` for each user on the device.

Content is available where security hardening content is available and is native to Management suites and MDM tools.

Content also available here: https://github.com/ronc-LAemigre/macos-sec-config

Internal Only - General

NIST guidance on passwords starting at 5.1.1.1

https://pages.nist.gov/800-63-3/sp800-63b.html

Additional references:

- https://developer.apple.com/documentation/devicemanagement/passcode
- https://krypted.com/mac-security/programatically-setting-password-policies/
- https://www.macworld.co.uk/news/flaw-mac-t2-chip-passwords-3813616/

Note: The current method of creating and setting password policy is using the `pwpolicy -setglobalpolicy` command. That command has been deprecated by Apple, but is still in use in the current version of macOS. The Benchmark will continue to use this command line method for passwords until Apple removes it from the OS. Setting password policy with mobile configuration profiles is the preferred method going forward.

Internal Only - General

5.2.1 Ensure Password Account Lockout Threshold Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

The account lockout threshold specifies the amount of times a user can enter an incorrect password before a lockout will occur.

Ensure that a lockout threshold is part of the password policy on the computer.

Rationale:

The account lockout feature mitigates brute-force password attacks on the system.

Impact:

The number of incorrect log on attempts should be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user log on.

The locked account will auto-unlock after a few minutes when bad password attempts stop. The computer will accept the still-valid password if remembered or recovered.

Audit:

Graphical Method:

Perform the following steps to ensure that the Password Account Threshold is set to less than or equal to 5 and the lockout time is greater than or equal to 15:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Max Failed Attempts` set to ≤ `5`

Terminal Method:

Run the following command to verify that the number of failed attempts is less than or equal to 5:

```
% /usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies 2> /dev/null |
/usr/bin/tail +2 | /usr/bin/xmllint --xpath
'//dict/key[text()="policyAttributeMaximumFailedAuthentications"]/following-
sibling::integer[1]/text()' -
```

The output should be ≤ `5`

Internal Only - General

Remediation:

Terminal Method:

Run the following command to set the maximum number of failed login attempts to less than or equal to 5:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"maxFailedLoginAttempts=<value≤5>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"maxFailedLoginAttempts=5"
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `maxFailedAttempts`
3. The key must be set to `<integer><value≤5></integer>`

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

Note: This is for the login password only and does not affect the timeout of FileVault.

References:

1. CIS Password Policy - https://workbench.cisecurity.org/communities/113
2. https://support.apple.com/guide/security/passcodes-and-passwords-sec20230a10d/web

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

Internal Only - General

5.2.2 Ensure Password Minimum Length Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

A minimum password length is the fewest number of characters a password can contain to meet a system's requirements.

Ensure that a minimum of a 15-character password is part of the password policy on the computer.

Where the confidentiality of encrypted information in FileVault is more of a concern, requiring a longer password or passphrase may be sufficient rather than imposing additional complexity requirements that may be self-defeating.

Rationale:

Information systems that are not protected with strong password schemes including passwords of minimum length provide a greater opportunity for attackers to crack the password and gain access to the system.

Impact:

Short passwords can be easily attacked.

Audit:

Graphical Method:

Perform the following steps to ensure that the Password Account Threshold is set to greater than or equal to 15:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `Min Password Length` set to ≥ `15`

Terminal Method:

Run the following command to verify that the password length is greater than or equal to 15:

```
/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -e
"policyAttributePassword matches" | /usr/bin/grep -e "[0-9][0-9]" |
/usr/bin/cut -b 46-53 | /usr/bin/cut -d',' -f1 | /usr/bin/cut -d'{' -f2
```

The output value should be ≥ `15`

Internal Only - General

Remediation:

Terminal Method:

Run the following command to set the password length to greater than or equal to 15:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"minChars=<value≥15>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"minChars=15"
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `minLength`
3. The key must be set to `<integer><value≥15></integer>`

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

5.2.3 Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Manual)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that an Alphabetic character is part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Graphical Method:

Perform the following steps to ensure that the passwords must contain at least 1 alphabetic character:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Requires Alphanumeric` set to `True`

Terminal Method:

Run the following command to verify that the password requires at least one letter:

```
% pref1=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-e "Contain at least one number and one alphabetic character." | cut -b 13-
68) && pref2=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies |
/usr/bin/grep -A1 minimumLetters | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2
| /usr/bin/cut -d '<' -f1) && if [ "$pref1" = "Contain at least one number
and one alphabetic character" ]; then echo "true"; elif [[ "$pref2" != "" &&
pref2 -ge 1 ]]; then echo "true"; else echo "false"; fi

true
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to set that passwords must contain at least one letter:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -
setaccountpolicies "requiresAlpha=<value≥1>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"requiresAlpha=1"
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `requireAlphanumeric`
3. The key must be set to `<true/>`

Note: This profile sets a requirement of both an alphabetical and a numeric character.

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations `5.3` - `5.6`). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

5.2.4 Ensure Complex Password Must Contain Numeric Character Is Configured (Manual)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that a number or numeric value is part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Graphical Method:

Perform the following steps to ensure that the passwords must contain at least 1 numeric character:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Requires Alphanumeric` set to `True`

Terminal Method:

Run the following command to verify that passwords require at least one number:

```
% pref1=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-e "Contain at least one number and one alphabetic character." | cut -b 13-
68) && pref2=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies |
/usr/bin/grep -A1 minimumNumericCharacters | /usr/bin/tail -1 | /usr/bin/cut
-d'>' -f2 | /usr/bin/cut -d '<' -f1) && if [ "$pref1" = "Contain at least one
number and one alphabetic character" ]; then echo "true"; elif [[ "$pref2" !=
"" && pref2 -ge 1 ]]; then echo "true"; else echo "false"; fi

true
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to set passwords to require at least one number:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -
setaccountpolicies "requiresNumeric=<value≥1>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"requiresNumeric=2"
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `requireAlphanumeric`
3. The key must be set to `<true/>`

Note: This profile sets a requirement of both an alphabetical and a numeric character.

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations `5.3` - `5.6`). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

5.2.5 Ensure Complex Password Must Contain Special Character Is Configured (Manual)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters. Ensure that a special character is part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Graphical Method:

Perform the following steps to ensure that the passwords must contain at least 1 special character:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Min Complex Length` set to ≥ `1`

Terminal Method:

Run the following command to verify that the password requires at least one special character:

```
% pref1=$(/usr/bin/sudo  /usr/bin/pwpolicy -getaccountpolicies |
/usr/bin/grep -e "policyAttributePassword matches '(.*[^a-zA-Z0-9].*){1,}'" |
cut -b 12-67) && pref2=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies
| /usr/bin/grep -A1 minimumSymbols | /usr/bin/tail -1 | /usr/bin/cut -d'>' -
f2 | /usr/bin/cut -d '<' -f1) && if [ "$pref1" = "policyAttributePassword
matches '(.*[^a-zA-Z0-9].*){1,}'" ]; then echo "true"; elif [[ "$pref2" != ""
&& pref2 -ge 1 ]]; then echo "true"; else echo "false"; fi

true
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to set passwords to require at least one special character:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -
setaccountpolicies "requiresSymbol=<value≥1>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"requiresSymbol=1"
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `minComplexChars`
3. The key must be set to `<integer><value≥1></integer>`

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations `5.3` - `5.6`). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

5.2.6 Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Manual)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that both uppercase and lowercase letters are part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Terminal Method:

Run the following command to verify that the password requires an upper and lower case letter:

```
% pref=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-A1 minimumMixedCaseCharacters | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 |
/usr/bin/cut -d '<' -f1) && if [[ "$pref" != "" && pref -ge 1 ]]; then echo
"true"; else echo "false"; fi

true
```

Remediation:

Terminal Method:

Run the following command to set passwords to require an upper and lower case letter:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"requiresMixedCase=<value≥1>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"requiresMixedCase=1"
```


Internal Only - General

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations 5.3 - 5.6). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

5.2.7 Ensure Password Age Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

Over time, passwords can be captured by third parties through mistakes, phishing attacks, third-party breaches, or merely brute-force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed), users should reset passwords periodically. This control uses 365 days as the acceptable value. Some organizations may be more or less restrictive. This control mainly exists to mitigate against password reuse of the macOS account password in other realms that may be more prone to compromise. Attackers take advantage of exposed information to attack other accounts.

Rationale:

Passwords should be changed periodically to reduce exposure.

Impact:

Required password changes will lead to some locked computers requiring admin assistance.

Audit:

Graphical Method:

Perform the following steps to ensure that the passwords expire after at most 365 days:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Max Age (days)` set to ≤ `365`

Internal Only - General

Terminal Method:

Run the following command to verify that the password expires after at most 365 days:

```
% pref1=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-A1 policyAttributeExpiresEveryNDays | /usr/bin/tail -1 | /usr/bin/cut -d'>'
-f2 | /usr/bin/cut -d '<' -f1) && pref2=$(/usr/bin/sudo /usr/bin/pwpolicy -
getaccountpolicies | /usr/bin/grep -A1 policyAttributeDaysUntilExpiration |
/usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 | /usr/bin/cut -d '<' -f1) && if [[
"$pref1" != "" && pref1 -le 365 ]]; then echo "true"; elif [[ "$pref2" != ""
&& pref2 -le 365 ]]; then echo "true"; else echo "false"; fi

true
```

Remediation:

Terminal Method:

Run the following command to require that passwords expire after at most 365 days:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"maxMinutesUntilChangePassword=<value≤525600>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"maxMinutesUntilChangePassword=43200"
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `maxPINAgeInDays`
3. The key must be set to `<integer><value≥365></integer>`

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	16.9 Disable Dormant Accounts Automatically disable dormant accounts after a set period of inactivity.	●	●	●

Internal Only - General

5.2.8 Ensure Password History Is Set to at least 24 (Automated)

Profile Applicability:

- Level 1

Description:

Over time, passwords can be captured by third parties through mistakes, phishing attacks, third-party breaches, or merely brute-force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed), users must reset passwords periodically. This control ensures that previous passwords are not reused immediately by keeping a history of previous password hashes. Ensure that password history checks are part of the password policy on the computer. This control checks whether a new password is different than the previous 24. The latest NIST guidance based on exploit research referenced in this section details how one of the greatest risks is password exposure rather than password cracking. Passwords should be changed to a new unique value whenever a password might have been exposed to anyone other than the account holder. Attackers have maintained persistent control based on predictable password change patterns and substantially different patterns should be used in case of a leak.

Rationale:

Old passwords should not be reused.

Impact:

Required password changes will lead to some locked computers requiring admin assistance.

Audit:

Graphical Method:

Perform the following steps to ensure that the password is not the same as at least the last 24 passwords:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `Max History Kept` set to ≥ `24`

Internal Only - General

Terminal Method:

Run the following command to verify that the password is required to be different from at least the last 24 passwords:

```
% pref=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-A1 policyAttributePasswordHistoryDepth | /usr/bin/tail -1 | /usr/bin/cut -
d'>' -f2 | /usr/bin/cut -d '<' -f1) && if [[ "$pref" != "" && pref -ge 1 ]];
then echo "true"; else echo "false"; fi

true
```

Remediation:

Terminal Method:

Run the following command to require that the password must be different from at least the last 24 passwords:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"usingHistory=<value≥24>"
```

example:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"usingHistory=24"
```

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.mobiledevice.passwordpolicy`
2. The key to include is `pinHistory`
3. The key must be set to `<integer><value≥24></integer>`

Note: The profile method is the preferred method for setting password policy since `-setglobalpolicy` in `pwpolicy` is deprecated and will likely be removed in a future macOS release.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

5.3 Encryption

Apple has created simple, easy-to-use encryption capabilities built into macOS. Those tools need to be utilized in order to protect information processed by macOS computers.

Internal Only - General

5.3.1 Ensure all user storage APFS volumes are encrypted (Manual)

Profile Applicability:

- Level 1

Description:

Apple developed a new file system which was first made available in 10.12 and then became the default in 10.13. The file system is optimized for Flash and Solid-State storage and encryption. https://en.wikipedia.org/wiki/Apple_File_System macOS computers generally have several volumes created as part of APFS formatting, including Preboot, Recovery and Virtual Memory (VM), as well as traditional user disks.

All APFS volumes that do not have specific roles and do not require encryption should be encrypted. "Role" disks include Preboot, Recovery and VM. User disks are labelled with "(No specific role)" by default.

Rationale:

In order to protect user data from loss or tampering volumes, carrying data should be encrypted.

Impact:

While FileVault protects the boot volume, data may be copied to other attached storage and reduce the protection afforded by FileVault. Ensure all user volumes are encrypted to protect data.

Audit:

Terminal Method:

Run the following command to list the APFS Volumes:

```
% /usr/bin/sudo /usr/sbin/diskutil ap list
```

Ensure all user data disks are encrypted.

Internal Only - General

example:

```
% /usr/bin/sudo /usr/sbin/diskutil ap list

APFS Volume Disk (Role):   disk1s1 (No specific role)
Name:                      Macintosh HD (Case-insensitive)
Mount Point:               /
Capacity Consumed:         188514598912 B (188.5 GB)
FileVault:                 Yes (Unlocked)

APFS Containers (2 found)
|
+-- Container disk1 XXXX
|   ==================================================
|   APFS Container Reference:     disk1
|   Size (Capacity Ceiling):      249152200704 B (249.2 GB)
|   Minimum Size:                 249152200704 B (249.2 GB)
|   Capacity In Use By Volumes:   195635597312 B (195.6 GB) (78.5% used)
|   Capacity Not Allocated:       53516603392 B (53.5 GB) (21.5% free)
|   |
|   +-< Physical Store disk0s4 XXXXXY
|   |   ----------------------------------------------------------
|   |   APFS Physical Store Disk:   disk0s4
|   |   Size:                       249152200704 B (249.2 GB)
|   |
|   +-> Volume disk1s1 XXXXXZ
|   |   ---------------------------------------------------
|   |   APFS Volume Disk (Role):   disk1s1 (No specific role)
|   |   Name:                      HighSierra (Case-insensitive)
|   |   Mount Point:               /
|   |   Capacity Consumed:         188514598912 B (188.5 GB)
|   |   FileVault:                 Yes (Unlocked)
|   |
|   +-> Volume disk1s2 XXXXXZZ
|   |   ---------------------------------------------------
|   |   APFS Volume Disk (Role):   disk1s2 (Preboot)
|   |   Name:                      Preboot (Case-insensitive)
|   |   Mount Point:               Not Mounted
|   |   Capacity Consumed:         23961600 B (24.0 MB)
|   |   FileVault:                 No
|   |
|   +-> Volume disk1s3 XXXXXYY
|   |   ---------------------------------------------------
|   |   APFS Volume Disk (Role):   disk1s3 (Recovery)
|   |   Name:                      Recovery (Case-insensitive)
|   |   Mount Point:               Not Mounted
|   |   Capacity Consumed:         518127616 B (518.1 MB)
|   |   FileVault:                 No
|   |
```


Internal Only - General

```
|   +-> Volume disk1s4 XXXXXYYY
|       ----------------------------------------------------
|       APFS Volume Disk (Role):   disk1s4 (VM)
|       Name:                      VM (Case-insensitive)
|       Mount Point:               /private/var/vm
|       Capacity Consumed:         6442704896 B (6.4 GB)
|       FileVault:                 No
|
+-- Container disk4 XXXXXYYYY
    ====================================================
    APFS Container Reference:     disk4
    Size (Capacity Ceiling):      119824367616 B (119.8 GB)
    Minimum Size:                 143192064 B (143.2 MB)
    Capacity In Use By Volumes:   126492672 B (126.5 MB) (0.1% used)
    Capacity Not Allocated:       119697874944 B (119.7 GB) (99.9% free)
    |
    +-< Physical Store disk3s2 XXXXXYYYYYY
    |   ------------------------------------------------------------
    |   APFS Physical Store Disk:   disk3s2
    |   Size:                       119824371200 B (119.8 GB)
    |
    +-> Volume disk4s1 C4D99580-1FDA-43BF-BB62-B21BF7EE568C
        ----------------------------------------------------
        APFS Volume Disk (Role):   disk4s1 (No specific role)
        Name:                      Passport (Case-insensitive)
        Mount Point:               /Volumes/Passport
        Capacity Consumed:         839680 B (839.7 KB)
        FileVault:                 Yes (Unlocked)
```

Remediation:

Use Disk Utility to erase a user disk and format as APFS (Encrypted).

Note: APFS Encrypted disks will be described as "FileVault" whether they are the boot volume or not in the ap list.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

Internal Only - General

5.3.2 Ensure all user storage CoreStorage volumes are encrypted (Manual)

Profile Applicability:

- Level 1

Description:

Apple introduced CoreStorage with Mac OS X 10.7 Lion. It is used as the default for formatting on macOS volumes prior to macOS 10.13 High Sierra.

All HFS and CoreStorage Volumes should be encrypted.

CoreStorage has been deprecated and replaced with APFS for volume encryption.

Rationale:

In order to protect user data from loss or tampering, volumes carrying data should be encrypted.

Impact:

While FileVault protects the boot volume, data may be copied to other attached storage and reduce the protection afforded by FileVault. Ensure all user volumes are encrypted to protect data.

Audit:

Terminal Method:

Run the following command to list the CoreStorage Volumes:

```
% /usr/bin/sudo /usr/sbin/diskutil cs list
```

Ensure all "Logical Volume Family" disks are encrypted

Internal Only - General

example:

```
% /usr/bin/sudo /usr/sbin/diskutil cs list

CoreStorage logical volume groups (2 found)
|
+-- Logical Volume Group XXXXX
|   =========================================================
|   Name:         Macintosh HD
|   Status:       Online
|   Size:         250160967680 B (250.2 GB)
|   Free Space:   6516736 B (6.5 MB)
|   |
|   +-< Physical Volume XXXXXY
|   |   ----------------------------------------------------
|   |   Index:    0
|   |   Disk:     disk0s2
|   |   Status:   Online
|   |   Size:     250160967680 B (250.2 GB)
|   |
|   +-> Logical Volume Family XXXXXYY
|       ----------------------------------------------------------
|       Encryption Type:         AES-XTS
|       Encryption Status:       Unlocked
|       Conversion Status:       Complete
|       High Level Queries:      Fully Secure
|       |                        Passphrase Required
|       |                        Accepts New Users
|       |                        Has Visible Users
|       |                        Has Volume Key
|       |
|       +-> Logical Volume XXXXXYYY
|           ----------------------------------------------------
|           Disk:                  disk2
|           Status:                Online
|           Size (Total):          249802129408 B (249.8 GB)
|           Revertible:            Yes (unlock and decryption required)
|           LV Name:               Macintosh HD
|           Volume Name:           Macintosh HD
|           Content Hint:          Apple_HFS
|
+-- Logical Volume Group XXXXXYYYY
    =========================================================
    Name:         Passport
    Status:       Online
    Size:         119690149888 B (119.7 GB)
    Free Space:   1486848 B (1.5 MB)
    |
```


Internal Only - General

```
    +-< Physical Volume XXXXXYYY
    |   ----------------------------------------------------
    |   Index:    0
    |   Disk:     disk3s2
    |   Status:   Online
    |   Size:     119690149888 B (119.7 GB)
    |
    +-> Logical Volume Family XXXXXYYYYY
        ----------------------------------------------------------
        Encryption Type:         AES-XTS
        Encryption Status:       Unlocked
        Conversion Status:       Complete
        High Level Queries:      Fully Secure
        |                        Passphrase Required
        |                        Accepts New Users
        |                        Has Visible Users
        |                        Has Volume Key
        |
        +-> Logical Volume XXXXXYYYYYY
            ---------------------------------------------------
            Disk:                  disk4
            Status:                Online
            Size (Total):          119336337408 B (119.3 GB)
            Revertible:            No
            LV Name:               Passport
            Volume Name:           Passport
            Content Hint:          Apple_HFS
```

Remediation:

Use Disk Utility to erase a disk and format as macOS Extended (Journaled, Encrypted).

References:

1. https://www.ufsexplorer.com/articles/storage-technologies/apple-core-storage/

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 Encrypt Data on Removable Media Encrypt data on removable media.		●	●
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

Internal Only - General

5.4 Ensure the Sudo Timeout Period Is Set to Zero (Automated)

Profile Applicability:

- Level 1

Description:

The sudo command allows the user to run programs as the root user. Working as the root user allows the user an extremely high level of configurability within the system. This control, along with the control to use a separate timestamp for each tty, limits the window where an unauthorized user, process, or attacker could utilize legitimate credentials that are valid for longer than required.

Rationale:

The `sudo` command stays logged in as the root user for five minutes before timing out and re-requesting a password. This five-minute window should be eliminated since it leaves the system extremely vulnerable. This is especially true if an exploit were to gain access to the system, since they would be able to make changes as a root user.

Impact:

This control has a serious impact where users often have to use sudo. It is even more of an impact where users have to use sudo multiple times in quick succession as part of normal work processes. Organizations with that common use case will likely find this control too onerous and are better to accept the risk of not requiring a 0 grace period.

In some ways the use of sudo -s, which is undesirable, is better than a long grace period since that use does change the hash to show that it is a root shell rather than a normal shell where sudo commands will be implemented without a password.

Audit:

Terminal Method:

Perform the following to verify the sudo timeout period:

```
$ /usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Authentication timestamp
timeout: 0.0 minutes"

1
```

Run the following commands to verify that the root is the owner of the `/etc/sudoers.d` folder, and that wheel is the group:

```
% /usr/bin/stat /etc/sudoers.d

16777229 19662948 drwxr-xr-x 2 root wheel 0 64 "Jun  7 23:12:24 2022" "May  9
17:30:48 2022" "Jun  7 23:12:24 2022" "May  9 17:30:48 2022" 4096 0 0
/etc/sudoers.d
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to edit the sudo settings:

```
% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/<configuration file name>
```

example: `% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/10_cissudoconfiguration`

Note: Unlike other Unix and/or Linux distros, macOS will ignore configuration files in the sudoers.d folder that contain a `.` so do not add a file extension to the configuration file.

Add the line `Defaults timestamp_timeout=0` to the configuration file.

If /etc/sudoers.d/ is not owned by root or in the wheel group, run the following to change ownership and group:

```
% /usr/bin/sudo /usr/sbin/chown -R root:wheel /etc/sudoers.d/
```

Additional Information:

In previous iterations and OS versions of the macOS Benchmark, the guidance was to edit the sudoers file directly. While this would properly configure the OS, any update would change the settings back to the default configuration. Creating a configuration file in the `/etc/sudoers.d/` folder will not be modified on an OS update and will keep the proper configuration.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

5.5 Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated)

Profile Applicability:

- Level 1

Description:

Using tty tickets ensures that a user must enter the sudo password in each Terminal session.

With sudo versions 1.8 and higher, introduced in 10.12, the default value is to have tty tickets for each interface so that root access is limited to a specific terminal. The default configuration can be overwritten or not configured correctly on earlier versions of macOS.

Rationale:

In combination with removing the sudo timeout grace period, a further mitigation should be in place to reduce the possibility of a background process using elevated rights when a user elevates to root in an explicit context or tty.

Additional mitigation should be in place to reduce the risk of privilege escalation of background processes.

Impact:

This control should have no user impact. Developers or installers may have issues if background processes are spawned with different interfaces than where sudo was executed.

Audit:

Terminal Method:

Run the following commands to verify that the default sudoers controls are in place with explicit tickets per tty:

```
% /usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Type of authentication
timestamp record: tty"

1
```


Internal Only - General

Remediation:

Terminal Method:

Run the following command to edit the sudo settings:

```
% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/<configuration file name>
```

example: `% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/10_cissudoconfiguration`

Note: Unlike other Unix and/or Linux distros, macOS will ignore configuration files in the sudoers.d folder that contain a `.` so do not add a file extension to the configuration file.

Add the line `Defaults timestamp_type=tty` to the configuration file.

Note: The `Defaults timestamp_type=tty` line can be added to an existing configuration file or a new one. That will depend on your organization's preference and works either way.

Default Value:

If no value is set, the default value of tty_tickets enabled will be used.

References:

1. https://github.com/jorangreef/sudo-prompt/issues/33

Additional Information:

In previous iterations and OS versions of the macOS Benchmark, the guidance was to edit the sudoers file directly. While this would properly configure the OS, any update would change the settings back to the default configuration. Creating a configuration file in the `/etc/sudoers.d/` folder will not be modified on an OS update and will keep the proper configuration.

With the configuration file, there is no need to remove the `Defaults !tty_tickets` line from the `visudo` settings. The configuration file will take precedent.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

5.6 Ensure the "root" Account Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The root account is a superuser account that has access privileges to perform any actions and read/write to any file on the computer. With some versions of Linux, the system administrator may commonly use the root account to perform administrative functions.

Rationale:

Enabling and using the root account puts the system at risk since any successful exploit or mistake while the root account is in use could have unlimited access privileges within the system. Using the `sudo` command allows users to perform functions as a root user while limiting and password protecting the access privileges. By default the root account is not enabled on a macOS computer. An administrator can escalate privileges using the `sudo` command (use `-s` or `-i` to get a root shell).

Impact:

Some legacy POSIX software might expect an available root account.

Audit:

Graphical Method:

Perform the following steps to ensure that the root user is not enabled:

1. Open `/System/Library/CoreServices/Applications/Directory Utility`
2. Click the lock icon to unlock the service
3. Click `Edit` in the `menu bar`
4. Verify that the menu shows `Enable Root User`, not `Disable Root User`

Internal Only - General

Terminal Method:

Run the following command to verify the the root user has not been enabled:

```
% /usr/bin/sudo /usr/bin/dscl . -read /Users/root AuthenticationAuthority


No such key: AuthenticationAuthority
```

Run the following command to verify the root shell is disabled:

```
%  /usr/bin/dscl . -read /Users/root UserShell 2>&1 | /usr/bin/grep -c
"/usr/bin/false"

1
```

Remediation:

Graphical Method:

Perform the following steps to ensure that the root user is disabled:

1. Open `/System/Library/CoreServices/Applications/Directory Utility`
2. Click the lock icon to unlock the service
3. Click `Edit` in the `menu bar`
4. Click `Disable Root User`

Terminal Method:

Run the following command to disable the root user:

```
% /usr/bin/sudo /usr/sbin/dsenableroot -d

username = root
user password:
```

Run the following command to disable the root user shell:

```
% /usr/bin/dscl . -create /Users/root UserShell /usr/bin/false
```


Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

Internal Only - General

5.7 Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session (Automated)

Profile Applicability:

- Level 1

Description:

macOS has a privilege that can be granted to any user that will allow that user to unlock active users' sessions.

Note: For organizations that are using Platform Single-Sign-On (PSSO), this setting can cause issues with syncing with your PSSO. See the note in the audit to verify if you are using PSSO.

Rationale:

Disabling the administrator's and/or user's ability to log into another user's active and locked session prevents unauthorized persons from viewing potentially sensitive and/or personal information.

Impact:

While Fast user switching is a workaround for some lab environments, especially where there is even less of an expectation of privacy, this setting change may impact some maintenance workflows.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify that a user cannot log into another user's active and/or locked session:

```
% /usr/bin/sudo /usr/bin/security authorizationdb read
system.login.screensaver 2>&1 | /usr/bin/awk -F "[<>]" '$3=="authenticate-
session-owner" { ++x } END { print x+0 }';

1
```

Note: To verify if your organization is using PSSO, run the following command:

```
% /usr/bin/sudo app-sso platform -s
```

If your output is:

```
Time: 2025-06-27 13:28:59 +0000

Device Configuration:
 (null)

Login Configuration:
 (null)

User Configuration:
 (null)
```

Your organization is not using PSSO and needs to remediate if not in alignment with the recommendation.

If the command outputs configuration information, do not apply the remediation.

Remediation:

Terminal Method:

Run the following command to disable a user logging into another user's active and/or locked session:

```
% /usr/bin/sudo /usr/bin/security authorizationdb write
system.login.screensaver authenticate-session-owner

YES (0)
```

Running this command will disable Touch ID to unlock the screen saver. To re-enable Touch ID for users, run the following command:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow screenUnlockMode -int 1
```


Internal Only - General

References:

1. https://derflounder.wordpress.com/2014/02/16/managing-the-authorization-database-in-os-x-mavericks/
2. https://www.jamf.com/jamf-nation/discussions/18195/system-login-screensaver

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

5.8 Ensure a Login Window Banner Exists (Automated)

Profile Applicability:

- Level 2

Description:

A Login window banner warning informs the user that the system is reserved for authorized use only. It enforces an acknowledgment by the user that they have been informed of the use policy in the banner if required. The system recognizes either the `.txt` and the `.rtf` formats.

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Impact:

Users will have to click on the window with the Login text before logging into the computer.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify the login window text:

```
% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.*
```

If the output includes `no matches found: /Library/Security/PolicyBanner.*` the system is not compliant.

Run the following to verify permissions of the policy banner file:

```
% /usr/bin/stat -f %A /Library/Security/PolicyBanner.*
```

The output should have `4` as the 3rd digit.

If there is an output, then the policy banner will not display.

example:

```
% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.txt

Center for Internet Security Test Message

% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.rtf

{\rtf1\ansi\ansicpg1252\cocoartf1561\cocoasubrtf610
{\fonttbl\f0\fswiss\fcharset0 Helvetica;}
{\colortbl;\red255\green255\blue255;}
{\*\expandedcolortbl;;}
\margl1440\margr1440\vieww10800\viewh8400\viewkind0
\pard\tx566\tx1133\tx1700\tx2267\tx2834\tx3401\tx3968\tx4535\tx5102\tx5669\tx
6236\tx6803\pardirnatural\partightenfactor0

\f0\fs24 \cf0 Center for Internet Security Test Message}

% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.*

{\rtf1\ansi\ansicpg1252\cocoartf1561\cocoasubrtf610
{\fonttbl\f0\fswiss\fcharset0 Helvetica;}
{\colortbl;\red255\green255\blue255;}
{\*\expandedcolortbl;;}
\margl1440\margr1440\vieww10800\viewh8400\viewkind0
\pard\tx566\tx1133\tx1700\tx2267\tx2834\tx3401\tx3968\tx4535\tx5102\tx5669\tx
6236\tx6803\pardirnatural\partightenfactor0

\f0\fs24 \cf0 Center for Internet Security Test Message}Center for Internet
Security Test Message

% /usr/bin/sudo stat -f %A /Library/Security/PolicyBanner.*

644
```


Internal Only - General

Remediation:

Terminal Method:

Run the following commands to create or edit the login window text and set the proper permissions:

Edit (or create) a `PolicyBanner.txt` or `PolicyBanner.rtf` file, in the `/Library/Security/` folder, to include the required login window banner text.

Perform the following to set permissions on the policy banner file:

```
% /usr/bin/sudo /bin/chmod o+r /Library/Security/PolicyBanner.txt

% /usr/bin/sudo /bin/chmod o+r /Library/Security/PolicyBanner.rtf
```

Note: If your organization uses an `.rtfd` file to set the policy banner, run `% /usr/bin/sudo /bin/chmod o+rx /Library/Security/PolicyBanner.rtfd` to update the permissions.

References:

1. https://support.apple.com/en-au/HT202277

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

5.9 Ensure the Guest Home Folder Does Not Exist (Automated)

Profile Applicability:

- Level 1

Description:

In the previous two controls, the guest account login has been disabled and sharing to guests has been disabled, as well. There is no need for the legacy Guest home folder to remain in the file system. When normal user accounts are removed, you have the option to archive it, leave it in place, or delete. In the case of the guest folder, the folder remains in place without a GUI option to remove it. If at some point in the future a Guest account is needed, it will be re-created. The presence of the Guest home folder can cause automated audits to fail when looking for compliant settings within all User folders, as well. Rather than ignoring the folder's continued existence, it is best removed.

Rationale:

The Guest home folders are unneeded after the Guest account is disabled and could be used inappropriately.

Impact:

The Guest account should not be necessary after it is disabled, and it will be automatically re-created if the Guest account is re-enabled

Audit:

Terminal Method:

Run the following command to verify if the Guest user home folder exists:

```
% /usr/bin/sudo /bin/ls /Users/ | /usr/bin/grep Guest
```

Note: This audit is looking for the folder titled `Guest`. If there are other folders in `/Users` that contain the word `Guest` within them, that is not necessarily a finding.

Remediation:

Terminal Method:

Run the following command to remove the Guest user home folder:

```
% /usr/bin/sudo /bin/rm -R /Users/Guest
```

Note: If the `Guest` folder exists it maybe a legacy folder. If so, the folder should be removed. If you are unsure if the `Guest` folder is a legacy folder, then your organization should research why that folder is there. Also research what is contained (or was contained) within it before removing the folder.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

5.10 Ensure XProtect Is Running and Updated (Automated)

Profile Applicability:

- Level 1

Description:

XProtect is Apple's native signature-based antivirus technology. XProtect both finds and blocks the execution of known malware. There are many AV and Endpoint Detection and Response (EDR) tools available for macOS. The native Apple provisioned tool looks for specific known malware and is completely integrated into the OS. No matter what other tools are being used, XProtect should have the latest signatures available.

Rationale:

Apple creates signatures for known malware that actually affects Macs and that knowledge should be leveraged.

Impact:

Some organizations may have effective macOS anti-malware tools that XProtect conflicts with.

Internal Only - General

Audit:

Terminal Method:

Run the following command to verify that XProtect is running and up-to-date:

```
% /usr/bin/sudo /usr/bin/xprotect status

XProtect launch scans: enabled
XProtect background scans: enabled
```

Note: XProtect can only be disabled while SIP (System Integrity Protection) is disabled. If XProtect is disabled while SIP is enabled, there needs to be a more significant investigation on this system and assume it is compromised in some way.

To verify the updates to XProtect, run the following commands:

```
% /usr/bin/sudo /usr/bin/xprotect check
```

The output will be `Current update: date:` with the date of the latest version and `version:` with the version number, ex. `Current update: date: 2025-07-01 19:55:44 +0000 version: 5303`. The `check` function can take a few minutes to verify the most up-to-date version of XProtect, so waiting 10+ minutes to run the next command is a best practice for verifying if XProtect is running the current version.

```
% /usr/bin/sudo /usr/bin/xprotect update

Starting update.
No update applied, already up to date
```

Remediation:

Terminal Method:

Run the following command to enable and update XProtect:

```
% /usr/bin/sudo /bin/launchctl load -w
/Library/Apple/System/Library/LaunchDaemons/com.apple.XProtect.daemon.scan.pl
ist

% /usr/bin/sudo /bin/launchctl load -w
/Library/Apple/System/Library/LaunchDaemons/com.apple.XprotectFramework.Plugi
nService.plist

% /usr/bin/sudo /usr/bin/xprotect update

Starting update.
Update succeeded: Activated update LocalUpdate[<newest XProtect version>]
```

Note: XProtect can only be enabled/disabled if SIP (System Integrity Protection) is disabled. If XProtect is disabled, the system might be compromised and needs to be investigated.

Internal Only - General

References:

1. https://eclecticlight.co/2021/10/27/silently-updated-security-data-files-in-monterey/
2. https://eclecticlight.co/2020/12/14/silently-updated-security-data-files-in-big-sur/
3. https://eclecticlight.co/2019/10/17/security-data-files-how-theyve-changed-in-catalina/
4. https://eclecticlight.co/2022/05/12/apple-has-pushed-an-update-to-xprotect-21/
5. https://support.apple.com/guide/security/protecting-against-malware-sec469d47bd8/web
6. https://eclecticlight.co/2023/06/12/malware-detection-and-remediation-by-xprotect-remediator/

Additional Information:

To verify the XProtect Remediator logs run the following command:

```
% /usr/bin/sudo /usr/bin/log show --predicate 'subsystem ==
"com.apple.XProtectFramework.PluginAPI" AND category ==
"XPEvent.structured"' --info --last 1d' to check logs'
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●

Internal Only - General

5.11 Ensure Logging Is Enabled for Sudo (Automated)

Profile Applicability:

- Level 1

Description:

In order to properly monitor the use of the `sudo` command, logs events for any use of `sudo` should be captured in the unified log.

Rationale:

Apple added sudo logging as part of the unified log in macOS 14.0 Sonoma. In macOS 15.0 Sequoia, it is now disabled by default but it should be enabled.

Impact:

Sensitive date (ex proprietary data, PII, etc) could be sent to the unified log with sudo logging enabled.

Audit:

Terminal Method:

Run the following commands to verify that the default sudoers controls are in place for logging of sudo commands:

```
% /usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Log when a command is
allowed by sudoers"

1
```

Remediation:

Terminal Method:

Run the following command to edit the sudo settings:

```
% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/<configuration file name>
```

example: `% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/10_cissudoconfiguration`

Note: Unlike other Unix and/or Linux distros, macOS will ignore configuration files in the sudoers.d folder that contain a `.` so do not add a file extension to the configuration file.

Add the line `Defaults log_allowed` to the configuration file.

Note: The `Defaults log_allowed` line can be added to an existing configuration file or a new one. That will depend on your organization's preference and works either way.

Internal Only - General

Default Value:

If no value is set, the default value of logging disabled will be used.

References:

1. https://github.com/jorangreef/sudo-prompt/issues/33

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

6 Applications

All Operating System default installs include OS vendor applications, or vendor endorsed channels. Most of these applications do not require explicit security controls as part of an OS Benchmark or a separate Benchmark. When the application is OS-specific it is much more efficient to include security guidance as part of the OS Benchmark where security controls are available. This section contains a small list of macOS applications where security controls exist and should be reviewed.

There is no insistence that any of the built-in applications must be used, as there are many alternative third party applications that may be used instead. Included applications are often core to the Operating System, and a lack of security controls will likely make the OS itself more vulnerable.

Internal Only - General

6.1 Finder

Internal Only - General

6.1.1 Audit Show All Filename Extensions (Manual)

Profile Applicability:

- Level 1

Description:

A filename extension is a suffix added to a base filename that indicates the base filename's file format. This is intended for any user that logs into the GUI and has a home folder and not for service accounts. For the audit, we will continue to verify that every account with a home folder has filename extensions enabled.

In macOS 15.0 Sequoia, the `Show all filename extensions` no longer worked consistently but does nominally default to showing all filename extensions. Due to this, the recommendation has been modified to audit this setting, but it is remaining in the benchmark as a good security practice to train users to verify that the file they are opening is the correct and expected filetype.

Rationale:

Visible filename extensions allow the user to identify the file type and the application it is associated with which leads to quick identification of misrepresented malicious files.

Impact:

The user of the system can open files of unknown or unexpected filetypes if the extension is not visible.

Audit:

Graphical Method:

Perform the following steps to ensure that file extensions are shown:

1. Open `Finder`
2. Select `Finder` in the `menu bar`
3. Select `Settings`
4. Select `Advanced`
5. Verify that `Show all filename extensions` is set

Internal Only - General

Terminal Method:

Run the following command to verify that displaying of file extensions is enabled:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults read
/Users/<username>/Library/Preferences/.GlobalPreferences.plist
AppleShowAllExtensions

1
```

example:

```
% /usr/bin/sudo -u firstuser /usr/bin/defaults read
/Users/firstuser/Library/Preferences/.GlobalPreferences.plist
AppleShowAllExtensions

1

% /usr/bin/sudo -u seconduser /usr/bin/defaults read
/Users/secondname/Library/Preferences/.GlobalPreferences.plist
AppleShowAllExtensions

The domain/default pair of
(/Users/secondname/Library/Preferences/.GlobalPreferences.plist,
AppleShowAllExtensions) does not exist
```

In this example, firstuser is in compliance and seconduser is not.

Remediation:

Graphical Method:

Perform the following steps to ensure file extensions are shown:

1. Open `Finder`
2. Select `Finder` in the `menu bar`
3. Select `Settings`
4. Select `Advanced`
5. Set `Show all filename extensions` to enabled

Internal Only - General

Terminal Method:

Run the following command to enable displaying of file extensions:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults write
/Users/<username>/Library/Preferences/.GlobalPreferences.plist
AppleShowAllExtensions -bool true

% /usr/bin/sudo killall Finder
```

example:

```
% /usr/bin/sudo -u seconduser /usr/bin/defaults write
/Users/secondname/Library/Preferences/.GlobalPreferences.plist
AppleShowAllExtensions -bool true

% /usr/bin/sudo killall Finder
```

Default Value:

Filename extensions are turned off by default.

References:

1. https://blog.xpnsec.com/macos-filename-homoglyphs-revisited/
2. https://null-byte.wonderhowto.com/how-to/hacking-macos-create-fake-pdf-trojan-with-applescript-part-2-disguising-script-0184706/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

Internal Only - General

6.2 Mail

Mail is Apple's OS-included email client on both macOS and iOS. It supports a range of email server services including iCloud, Exchange, Gmail and standard IMAP and POP accounts. With the vast barrage of phishing attacks, any Internet email client is an exploitable risk on a user system. Any email client should be hardened with controls that assist the user against social engineering attacks to reduce the risk of unwanted emails. This benchmark is not advocating for all users to use Apple Mail, just providing guidance on controls for the built-in email client. Other email clients will have their own set of security controls.

Apple provides a service for Apple+ users called "Hide My Email." With this service, Apple creates unique email addresses (@iCloud.com) for domains that ask for my email addresses which Apple forwards to your email address of record under your Apple Account. This feature reduces tracking capabilities for third parties.

What is Hide My Email?

What is Email Hashing? The Importance of Hashed Email for Future Success

Apple Mail fully supports S/MIME without the use of any third party plugin. While there are very few remaining trusted CAs issuing free S/MIME certificates, the use of a trusted CA and digital signing enables others to interact with you using end-to-end encryption through encrypted email. An internal CA may also be used but partner trust of the CA will have to be coordinated.

More S/MIME info

Sign or encrypt emails in Mail on Mac

Installing an S/MIME Certificate and Sending Secure Email in macOS

Obtaining and using an S/MIME certificate on Apple MacOS

Sources of Free S/MIME Certificates

Internal Only - General

6.2.1 Ensure Protect Mail Activity in Mail Is Enabled (Manual)

Profile Applicability:

- Level 2

Description:

Apple provides privacy protection that should be enabled for the mail app on macOS to reduce information collection from a user that receives email.

Rationale:

Email is routinely abused by attackers, spammers and marketers. The "Protect Mail Activity" control reduces risk by hiding the current IP address of your Mac and privately downloading remote content.

The Protect Mail Activity function of privately downloading remote content is not applicable for those users that do not download any remote content. Typical Internet email is no longer plain text and will not render properly without remote content. Personal email or mailing list email may function without complaint by blocking remote content.

Impact:

Some remote content may be access-controlled and refuse to download with this setting enabled.

Audit:

Graphical Method:

Perform the following steps to verify that protect mail activity is enabled:

1. Open `Mail`
2. Select `Mail` in the `menu bar`
3. Select `Settings...`
4. Select `Privacy`
5. Verify that `Protect Mail Activity` is enabled

Internal Only - General

Remediation:

Graphical Method:

Perform the following steps to enabled protect mail activity:

1. Open `Mail`
2. Select `Mail` in the `menu bar`
3. Select `Settings...`
4. Select `Privacy`
5. Set `Protect Mail Activity` to enabled

References:

1. https://support.apple.com/guide/mail/use-mail-privacy-protection-mlhl03be2866/mac

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●

Internal Only - General

6.3 Safari

Safari is Apple's included web browser. Many macOS services only operate, or operate more efficiently, through Safari's (and macOS's) use of WebKit frameworks, Javascript included. Javascript has become an essential part of the modern web, and should not be disabled for standard use cases.

https://www.apple.com/safari/

One Safari advantage over other browsers that must be mentioned is the integration of Safari with Apple Pay. With Apple's payment system users do not have to store credit cards with merchants or in insecure auto-fill mechanisms but relies on macOS encrypted storage to protect user information. Apple Pay also supports virtual credit cards that can be revoked as neccessary. It is possible to use Apple Pay with third party browsers but it is more complicated and involves authorization through a user's Apple iPhone. Information on using other browsers

Internal Only - General

6.3.1 Ensure Automatic Opening of Safe Files in Safari Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Safari will automatically run or execute what it considers safe files. This can include installers and other files that execute on the operating system. Safari evaluates file safety by using a list of filetypes maintained by Apple. The list of files include text, image, video and archive formats that would be run in the context of the OS rather than the browser.

Rationale:

Hackers have taken advantage of this setting via drive-by attacks. These attacks occur when a user visits a legitimate website that has been corrupted. The user unknowingly downloads a malicious file either by closing an infected pop-up or hovering over a malicious banner. An attacker can create a malicious file that will fall within Safari's safe file list that will download and execute without user input.

Impact:

Apple considers many files that the operating system itself auto-executes as "safe files." Many of these files could be malicious and could execute locally without the user even knowing that a file of a specific type had been downloaded.

Audit:

Graphical Method:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `AutoOpenSafeDownloads` set `0`

Terminal Method:

Run the following command to verify that a profile is installed that disables safe files from opening in Safari:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep AutoOpenSafeDownloads | /usr/bin/tr -d ' '

AutoOpenSafeDownloads = 0;
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Safari`
2. The key to include is `AutoOpenSafeDownloads`
3. The key must be set to: `<false/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●
v7	7.9 Block Unnecessary File Types Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.		●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

Internal Only - General

6.3.2 Audit History and Remove History Items (Manual)

Profile Applicability:

- Level 2

Description:

Organizational management of user web browsing history is a challenge affected by multiple facets. Organizations should decide whether to manage browser history and how much history should be maintained.

Rationale:

There are conflicting concerns in the retention of browser history. Unlimited retention:

- Consumes disk space
- Is preferred by on-disk forensics teams
- Is user searchable for old visited pages
- Raises some user privacy concerns
- Has security concerns regarding retaining old links that may be stale or lead to compromised pages, or pages with changes or inappropriate content

Old browser history becomes stale and the use or misuse of the data can lead to unwanted outcomes. Search engine results are maintained and often provide much more relevant current information than old website visit information.

Impact:

If old browsing history is not available, it will not be available to authorized or unauthorized users. Some users may find old and even stale information useful.

Audit:

Graphical Method:

Perform the following steps to verify how long the history in Safari is kept:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `HistoryAgeInDaysLimit` set to your organization's requirements

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that sets how long the history is kept in Safari:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep HistoryAgeInDaysLimit | /usr/bin/tr -d ' '
```

The output will be `HistoryAgeInDaysLimit =` followed by your organizations requirements.

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Safari`
2. The key to include is `HistoryAgeInDaysLimit`
3. The key must be set to: `<integer><1,7,14,31,365,36500></integer>`

Note: Setting the plist key to a value that is not represented by the GUI could cause issues.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●

Internal Only - General

6.3.3 Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple uses the Google Safe Browsing API to check for fraudulent websites and report them to the user attempting to visit one.

Rationale:

Attackers use crafted web pages to social engineer users to load unwanted content. Warning users prior to loading the content enables better security.

Impact:

Once-compromised websites serving malware could be sanitized and remain in the database, though there is no widespread reporting of that risk.

Audit:

Graphical Method:

Perform the following to verify that warn when visiting a fraudulent site in Safari is enabled:

1. Open `System Preferences`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `WarnAboutFraudulentWebsites` set to `1`

Terminal Method:

Run the following command to verify that a profile is installed that warns when visiting fraudulent sites in Safari:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep WarnAboutFraudulentWebsites | /usr/bin/tr -d ' '

WarnAboutFraudulentWebsites = 1;
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Safari`
2. The key to include is `WarnAboutFraudulentWebsites`
3. The key must be set to: `<true/>`

References:

1. https://support.apple.com/guide/safari/security-ibrw1074/16.0/mac/12.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●

Internal Only - General

6.3.4 Ensure Prevent Cross-site Tracking in Safari Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

There is a vast network of groups that collect, use, and sell user data. One method used to collect user data is pay and provide content and services for website owners. Along with that "assistance," the site owners also push tracking cookies on visitors. In many cases the help allows a content owner to keep the site up. The tracking cookies allow information brokers to track web users across visited sites. For better privacy and to provide some resistance to data brokers, prevent cross-tracking.

Rationale:

Cross-tracking allows data-brokers to follow you across the Internet to enable their business model of selling personal data. Users should protect their data and not volunteer it to marketing companies.

Impact:

Marketing companies will be unable to target you as effectively.

Audit:

Graphical Method:

Perform the following to verify that preventing cross-site tracking in Safari is enabled:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `BlockStoragePolicy` set to `2`
5. Verify that an installed profile also has `WebKitPreferences.storageBlockingPolicy` set to `1`
6. Verify that an installed profile also has `WebKitStorageBlockingPolicy` set to `1`

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that prevents cross-site tracking in Safari:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep BlockStoragePolicy | /usr/bin/tr -d ' '

BlockStoragePolicy = 2;

% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep WebKitPreferences.storageBlockingPolicy | /usr/bin/tr -d ' '

WebKitPreferences.storageBlockingPolicy = 1;

% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep WebKitStorageBlockingPolicy | /usr/bin/tr -d ' '

WebKitStorageBlockingPolicy = 1;
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Safari`
2. The key to include is `BlockStoragePolicy`
3. The key must be set to: 2
4. The key to also include is `WebKitPreferences.storageBlockingPolicy`
5. The key must be set to: 1
6. The key to also include is `WebKitStorageBlockingPolicy`
7. The key must be set to: 1

Internal Only - General

References:

1. https://support.apple.com/guide/safari/prevent-cross-site-tracking-sfri40732/mac

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●

Internal Only - General

6.3.5 Audit Hide IP Address in Safari Setting (Manual)

Profile Applicability:

- Level 2

Description:

Public (Routable) IP addresses can be used to track people to their current location, including home and business addresses. While a valid IP address is necessary to load the site, the valid address does not need to be provided to known trackers and should be hidden.

Rationale:

Trackers can correlate your visits through various applications, including websites, and are a threat to your privacy.

Impact:

Website address blocking through iCloud Private Relay may prevent some wanted pages from loading that use IP geolocation access controls.

Some organizations use IP address access controls (ACLs). If your organization or partners are using IP address ACLs, there will be unreachable web services if Apple hides the IP address.

Audit:

Graphical Method:

Perform the following steps to verify the setting for hiding IP addresses from trackers in Safari:

1. Open `Safari`
2. Select `Safari` from the `menu bar`
3. Select `Settings`
4. Select `Privacy`
5. Verify that `Hide IP address from trackers` is set to your organization's requirement

Internal Only - General

Terminal Method:

Run the following command to verify if IP addresses are hidden from trackers in Safari:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults read
/Users/<username>/Library/Containers/com.apple.Safari/Data/Library/Preference
s/com.apple.Safari WBSPrivacyProxyAvailabilityTraffic
```

The output will be either `33422560` if hide IP address from trackers is disabled, `33422564` if enabled from Trackers Only, or `33422572` if enabled from Trackers and Websites.

example:

```
% /usr/bin/sudo -u firstuser /usr/bin/defaults read
/Users/firstuser/Library/Containers/com.apple.Safari/Data/Library/Preferences
/com.apple.Safari WBSPrivacyProxyAvailabilityTraffic

130272

% /usr/bin/sudo -u seconduser /usr/bin/defaults read
/Users/seconduser/Library/Containers/com.apple.Safari/Data/Library/Preference
s/com.apple.Safari WBSPrivacyProxyAvailabilityTraffic

130276
```

In the above example the firstuser has hide ip address from trackers disabled. Seconduser has it enabled.

Note: To run the Terminal commands, Terminal must be granted Full Disk Access in the Security & Privacy pane in System Preferences.

Remediation:

Graphical Method:

Perform the following steps to set Safari whether or not to hide IP addresses from trackers:

1. Open `Safari`
2. Select `Safari` from the `menu bar`
3. Select `Settings`
4. Select `Privacy`
5. Set `Hide IP address from trackers` to your organization's requirements

Internal Only - General

Terminal Method:

Run the following command to enable or disable hiding IP addresses from trackers in Safari:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults write
/Users/<username>/Library/Containers/com.apple.Safari/Data/Library/Preference
s/com.apple.Safari WBSPrivacyProxyAvailabilityTraffic -int <130272/130276>
```

33422560 will set hide IP address from trackers to disabled. 33422564 will enable from Trackers Only, and 33422572 will enabled from Trackers and Websites.

example:

```
% /usr/bin/sudo -u firstuser /usr/bin/defaults write
/Users/firstuser/Library/Containers/com.apple.Safari/Data/Library/Preferences
/com.apple.Safari WBSPrivacyProxyAvailabilityTraffic -int 33422560

% /usr/bin/sudo -u seconduser /usr/bin/defaults write
/Users/seconduser/Library/Containers/com.apple.Safari/Data/Library/Preference
s/com.apple.Safari WBSPrivacyProxyAvailabilityTraffic -int 33422564

% /usr/bin/sudo -u thirduser /usr/bin/defaults write
/Users/thirduser/Library/Containers/com.apple.Safari/Data/Library/Preferences
/com.apple.Safari WBSPrivacyProxyAvailabilityTraffic -int 33422572
```

Note: To run the Terminal commands, Terminal must be granted Full Disk Access in the Security & Privacy pane in System Preferences.

References:

1. https://support.apple.com/en-bn/guide/safari/sfri35610/16.0/mac/12.0

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●

Internal Only - General

6.3.6 Ensure Advertising Privacy Protection in Safari Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple provides a framework that allows advertisers to target Apple users and end-users with advertisements. While many people prefer that when they see advertising it is relevant to them and their interests, the detailed information that is data mining collected, correlated, and available to advertisers in repositories is often disconcerting. This information is valuable to both advertisers and attackers and has been used with other metadata to reveal users' identities.

Organizations should manage advertising settings on computers rather than allow users to configure the settings.

Apple Information

Ad tracking should be limited on 10.15 and prior.

Rationale:

Organizations should manage user privacy settings on managed devices to align with organizational policies and user data protection requirements.

Impact:

Uses will see generic advertising rather than targeted advertising. Apple warns that this will reduce the number of relevant ads.

Audit:

Graphical Method:

Perform the following steps to verify that allow privacy-preserving measurement of ad effectiveness in Safari is enabled:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `WebKitPreferences.privateClickMeasurementEnabled` set `1`

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that disables safe files from opening in Safari:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep "WebKitPreferences.privateClickMeasurementEnabled" |
/usr/bin/tr -d ' '

"WebKitPreferences.privateClickMeasurementEnabled" = 1;
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Safari`
2. The key to include is `WebKitPreferences.privateClickMeasurementEnabled`
3. The key must be set to: `<true/>`

Note: A user can still uncheck this option in the GUI, but it remains on in the background and will show it enabled when re-launching Safari.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●

Internal Only - General

6.3.7 Ensure Show Full Website Address in Safari Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Attackers use websites with malicious or unwanted content to exploit the user or the computer. Part of the attack chain is to lure someone to load their content rather than the desired content. In order to reduce the risk in interacting with unwanted content, the full website address should always be displayed in Safari.

Rationale:

Full visibility into what site is being visited is important for privacy and security.

Impact:

Many URLs are very long and complicated, particularly for internal content management systems. Some complete URLS in the Smart Search Field may be difficult to parse.

Audit:

Graphical Method:

Perform the following steps to verify that showing full website addresses in Safari is enabled:

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `ShowFullURLInSmartSearchField` set `1`

Terminal Method:

Run the following command to verify that a profile is installed that disables safe files from opening in Safari:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep ShowFullURLInSmartSearchField | /usr/bin/tr -d ' '

ShowFullURLInSmartSearchField = 1;
```


Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Safari`
2. The key to include is `ShowFullURLInSmartSearchField`
3. The key must be set to: `<true/>`

References:

1. https://apple.stackexchange.com/questions/371473/always-show-full-url-in-safari-address-bar

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●

Internal Only - General

6.3.8 Audit AutoFill (Manual)

Profile Applicability:

- Level 2

Description:

AutoFill capabilities in a Web Browser are a feature to allow a user to avoid re-typing the same user information in every form that a user encounters. Part of the modern internet consists of vendors establishing a seemingly close relationship with as many users as possible to market to them, data-mine from them and sell their data to third-party data aggregators. AutoFill can be a method for a user to share too much information with untrusted website owners. Many security professionals advise disabling AutoFill to reduce the risk of over-sharing. These security professionals appear to believe that manual data entry is better, since completing the required forms are often the only method to connect to needed data. The best method for security is to ensure that the data ready to be auto-filled is an acceptable risk to sites a user interacts with. Users must review what data they accept the risk to share.

Rationale:

Auditing and accepting information a user is willing to share prior to loading the blank form is the best way to manage risk.

Impact:

A user could overshare information based on trusting a site more than required.

Audit:

Graphical Method:

Perform the following steps to verify AutoFill in Safari:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `safariAllowAutoFill` set to your organization's requirements

Internal Only - General

Terminal Method:

Run the following command to verify that a profile is installed that sets autofill in Safari to your organization's requirements:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('safariAllowAutoFill').js
EOS

false
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.applicationaccess`
2. The key to include is `safariAllowAutoFill`
3. The key must be set to `<<true>or<false>/>`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●

Internal Only - General

6.3.9 Audit Pop-up Windows (Manual)

Profile Applicability:

- Level 1

Description:

Browser pop-up windows have long been one of the most annoying delivery mechanisms of unwanted web content. The content can be unwanted content, including Not Safe For Work, or malicious content relying on a user interacting with the pop-up. Safari has a built-in capability to disable pop-ups that should be enabled.

Rationale:

Pop-up windows are almost always unwanted content and should be blocked.

Impact:

Obsolete web content delivery systems may still rely on pop-ups on internal web portals. Specific domains can be set to be allowed if absolutely necessary. Web Developers should update content to reduce risk in the environment so that no pop-ups are allowed.

Audit:

Graphical Method:

Perform the following to verify that the pop-up settings in Safari:

1. Open `Safari`
2. Select `Safari` from the `menu bar`
3. Select `Settings`
4. Select `Websites`
5. Select `Pop-up Windows`
6. Verify the websites listed in `Allow pop-up windows on the website below:` are allowed according to your organization's requirements
7. Verify that `When visiting other websites` is set to `Block and Notify` or `Block`

Internal Only - General

Remediation:

Graphical Method:

Perform the following to configure pop-ups in Safari:

1. Open `Safari`
2. Select `Safari` from the `menu bar`
3. Select `Settings`
4. Select `Websites`
5. Select `Pop-up Windows`
6. Set all websites to `Block and Notify` or `Block`, listed in `Allow pop-up windows on the website below:`, or select `Remove` to remove a website
7. Set that `When visiting other websites` is set to `Block and Notify` or `Block`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●

Internal Only - General

6.3.10 Ensure Show Status Bar Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

The Status Bar in Safari shows the full URL of any link on hover. It protects the user from visiting sites where the domain has been obfuscated by allowing the user to review whether the link points to an unexpected location.

Rationale:

Showing the Status Bar allows the user to review the full URL of hyperlinks.

Impact:

The Status Bar is only visible at the very bottom of the Web page when a hyperlink is hovered over. There should be no noticeable impact.

Audit:

Graphical Method:

Perform the following to verify that the status bar in Safari is enabled:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `ShowOverlayStatusBar` set to `1`

Terminal Method:

Run the following command to verify that a profile is installed that enables the status bar in Safari:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType |
/usr/bin/grep ShowOverlayStatusBar | /usr/bin/tr -d ' '

ShowOverlayStatusBar = 1;
```

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Safari`
2. The key to include is `ShowOverlayStatusBar`
3. The key must be set to: `<true/>`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	●	●	●

Internal Only - General

6.4 Terminal

Terminal is the Command Line Interface (CLI) for macOS.

Terminal User Guide

Internal Only - General

6.4.1 Ensure Secure Keyboard Entry Terminal.app Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Secure Keyboard Entry prevents other applications on the system and/or network from detecting and recording what is typed into Terminal. Unauthorized applications and malicious code could intercept keystrokes entered in the Terminal.

Rationale:

Enabling Secure Keyboard Entry minimizes the risk of a key logger detecting what is entered in Terminal.

Impact:

Enabling this in Terminal would prevent an application that is otherwise validly intercepting keyboard input from intercepting that input in Terminal.app. This could impact productivity tools.

Audit:

Graphical Method:

Perform the following steps to ensure that keyboard entries are secure in Terminal:

1. Open `System Settings`
2. Select `General`
3. Select `Device Management`
4. Verify that an installed profile has `SecureKeyboardEntry` is set to `1`

Terminal Method:

Run the following command to verify that a profile is installed that enables secure keyboard entry in Terminal:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.Terminal')\
.objectForKey('SecureKeyboardEntry').js
EOS

true
```

Note: Since the profile method sets a system-wide setting, the individual user audit and/or remediation has been removed. To be compliant, a profile must be installed for this recommendation. We have included the individual user information in the additional information section for reference only.

Internal Only - General

Remediation:

Profile Method:

Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.Terminal`
2. The key to include is `SecureKeyboardEntry`
3. The key must be set to `<true/>`

Note: Since the profile method sets a system-wide setting and not a user-level one, the profile method is the preferred method. It is always better to set system-wide than per user.

References:

1. https://support.apple.com/en-ca/guide/terminal/trml109/mac
2. https://developer.apple.com/library/archive/technotes/tn2150/_index.html
3. https://krypted.com/mac-os-x/secure-keyboard-entry-on-macos/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

6.5 Passwords

In macOS 15.0 Sequoia, Apple created the `Passwords` app to replace the existing `System Setting`.

Internal Only - General

6.5.1 Audit Passwords (Manual)

Profile Applicability:

- Level 1

Description:

Apple has provided a new interface in macOS Monterey for managing passwords that mirrors the interfaced capability already available in iOS. Password management in macOS was previously available in both Safari Preferences and in Keychain Access. Apple is attempting to simplify password management for macOS and make the user experience more similar to iOS. Organizations are justifiably concerned about the risk of password managers, particularly as a possible backdoor to improved credential management regimes and greater use of Multi-Factor-Authentication (MFA).

Apple has information posted on this system preference with additional information.

Change Passwords preferences on Mac

A warning icon is shown next to a website for any of the following reasons:

- Easily guessed
- Appeared in a data leak
- Reused on another website

Rationale:

Organizations should remove what passwords can be saved on user computers, thus limiting the ability of attackers to potentially steal organizational credentials. Limits on password storage must be evaluated based on both user risk and Enterprise risk.

Impact:

Organizations using passwords are constantly reported as having their password databases leaked to the Internet so every password a user has should be unique. Locking down secure password management solutions so that they cannot be used pushes users to password reuse, sticky notes, or always open text files with long lists of credentials.

Internal Only - General

Audit:

Graphical Method:

Perform the following steps to audit the Password system settings:

1. Open `Passwords`
2. Enter the user's password
3. Select `Security`
4. Verify that any recommendations or compromised passwords are set to match your organization's settings
5. Review applications with stored passwords to ensure that Enterprise managed passwords are not stored inappropriately. Application interfaces may need to be considered as well, as they allow the opportunity to store passwords that should not be saved.

Remediation:

Graphical Method:

Perform the following steps to set Password system settings to your organization's settings:

1. Open `Passwords`
2. Enter the user's password
3. Select the `Security`
4. Remove stored passwords that should not be saved.
5. Update any passwords that are compromised and are still in use by the organization.

References:

1. https://support.apple.com/guide/security/password-monitoring-sec78e79fc3b/1/web/1

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

7 Supplemental

This section is designed to give additional information on the security of macOS. There will be no specific guidance in the recommendations but it will include subjects that your organization should look into.

Internal Only - General

7.1 CIS Apple macOS Benchmark development collaboration with mSCP

The macOS Security Compliance Project (mSCP) is an open-source effort to provide a programmatic approach to generating security guidance. It is authoritative through the National Institute of Standards and Technology (NIST) Special Publication 800-219, Automated Secure Configuration Guidance from the mSCP.

This CIS Apple macOS 15 Sequoia Benchmark was developed as part of a working group collaboration with the mSCP and CIS writers and editors. The mSCP can be found at the macOS Security Compliance GitHub repository.

Internal Only - General

7.2 Apple Push Notification Service (APNs)

Apple Push Notification Service (APNs) is a platform notification service that allows third party developers to send notification data to applications installed on macOS (as well as iOS, iPadOS, watchOS, tvOS, and visionOS) devices. Mobile device management (MDM) tools can also utilize APNs to manage the devices enrolled in their service. APNs is an encrypted and authenticated communication protocol.

To learn more about APNs, read Apple's article entitled Use Apple products on enterprise networks.

Internal Only - General

7.3 Mobile Configuration Profiles

Mobile Configuration Profiles, or profiles for short, are XML files that consist of payloads to configure or authorize information for Apple devices. Profiles automate the configuration of settings, accounts, restrictions, and credentials. These files can be created by an MDM solution or Apple Configurator for Mac, or they can be created manually. To learn more about creating mobile configuration files, read Apple's support documentation on either MDM payload list for Mac computers or Profile-Specific Payload Keys.

The file must contain certain components for it to properly configure the operating system. An example can be found below:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>Key that is being set</key>
            <Value>
            <key>PayloadIdentifier</key>
            <string>com.example.myprofile</string>
            <key>PayloadType</key>
            <string>The PayloadType or what is being configured</string>
            <key>PayloadUUID</key>
            <string>This is a unique identifier for every profile and can be
created with the command /usr/bin/uuidgen</string>
            <key>PayloadVersion</key>
            <integer>1</integer>
        </dict>
    </array>
    <key>PayloadDisplayName</key>
    <string>The name that is displayed in System Settings</string>
    <key>PayloadIdentifier</key>
    <string>com.example.myprofile</string>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>This is another unique identifier and can be created with the
command /usr/bin/uuidgen</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
</plist>
```

Mobile configuration profiles must follow the names structure of `<filename>.mobileconfig`, ex `mypfrofile.mobileconfig` or `wifisettings.mobileconfig`.

Internal Only - General

7.4 Mobile Device Management (MDM) Software

Apple provides the capability to manage macOS, iOS, and iPadOS using Mobile Device Management (MDM) and is the preferred method to manage Apple devices. Profiles are used to configure devices to enforce security controls as well as to configure the devices for authorized access. Many security controls available on Apple devices are only available through the use of profile settings using MDM. This capability is also misused by attackers who have added rogue profiles to the list of unwanted software and fake software updates to induce users to approve the installation of malicious content. Organizations should have Mobile Device Management software in place to harden organizationally managed devices and take advantage of additional Apple controls, as well as to make the devices more resistant to attackers enticing users to install unwanted content from rogue MDMs.

Apple first announced Declarative Device Management at WWDC 2021 and has since confirmed that future management capabilities will specifically focus on the declarative management feature set.

Per Apple, "Declarative Device Management is an update to the existing protocol for device management that can be used in combination with the existing MDM protocol capabilities. It allows the device to asynchronously apply settings and report status back to the MDM solution without constant polling."

Organizations must ensure that their MDM solution supports this feature to utilize Declarative Device Management. Organizations interested in leveraging Declarative Device Management (DDM) must become familiar with its capabilities and how it will interact with other tools.

The Center for Internet Security does not endorse any particular MDM vendor or methodology for managing macOS devices. However, we aim to provide information for administrators, security specialists, auditors, help desk personnel, and platform deployment personnel involved in developing, deploying, assessing, or securing solutions incorporating Apple macOS 14.0 Sonoma.

A feature of Declarative Device Management is the ability to deploy "Legacy Declarative Configurations." You can use this configuration to download and install profiles with payloads unavailable as declarative configurations. In addition, Declarative Device Management now supports managing already installed MDM profiles without needing to remove them. An MDM server must send and activate a configuration containing the same profile as one already installed by MDM. The Declarative Device Management system will then take over the management of that profile without reinstalling or updating it. At that point, Declarative Device Management owns the profile. Using Legacy Declarative Configurations will result in the configuration data being written out to PLIST files, the same as a configuration profile. With Declarative Management taking over a configuration profile with Legacy Declarative Configurations, the MDM will not be able to make changes to it.

Internal Only - General

When implementing Declarative Device Management, MDM servers will write configuration data into an encrypted data container inaccessible to the device. The current state of a device's Declarative configuration and emitted status items will only be accessible by the MDM. Monitoring and auditing of the settings should be done on the local system against the state of the device.

Only the MDM solution can subscribe to the declarative status channel and reports of devices to be aware of the state of the configurations applied to the system. As a result, security and auditing solutions may have to query the MDM server directly for the state of configurations and compliance instead of scanning the local macOS system for this information. Because Configuration Profiles and Declarative Configurations may live side by side while Declarative Device Management becomes more widely adopted, organizations must decide which is best for the business and be mindful when utilizing both management features.

For macOS 14.0 Sonoma, implementing certain Declarative Configurations may affect the ability to perform auditing or remediation outlined within this benchmark. Organizations may be required to defer to their MDM solution for audit and validation. 1: Using Declarative Configuration Services: Utilizing this allows for managing System Integrity Protected (SIP) Services, including sshd, sudo, PAM, CUPS, Apache httpd, bash, and z-shell. *Affects (as labeled in Ventura Benchmark): CIS 2.3.3.4, CIS 2.3.3.5, CIS 4.2, CIS 5.4 2: Passcode/Password Policies. *Affects the entire 5.2 Password Management section (as labeled in Ventura Benchmark).

References:

- Intro to device management profiles
- Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
- CM-06 Configuration Settings
- MacOS Red Teaming 202: Profiles
- How to migrate macOS devices between MDMs
- Apple Platform Deployment
- Meet Declarative Device Management (WWDC21)
- Review declarative configurations for Apple devices

Internal Only - General

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Install Updates, Patches and Additional Security Software**		
1.1	Ensure Apple-provided Software Updates Are Installed (Automated)	☐	☐
1.2	Ensure Download New Updates When Available Is Enabled (Automated)	☐	☐
1.3	Ensure Install of macOS Updates Is Enabled (Automated)	☐	☐
1.4	Ensure Install Application Updates from the App Store Is Enabled (Automated)	☐	☐
1.5	Ensure Install Security Responses and System Files Is Enabled (Automated)	☐	☐
1.6	Ensure Software Update Deferment Is Less Than or Equal to 30 Days (Automated)	☐	☐
2	**System Settings**		
2.1	**Apple Account**		
2.1.1	**iCloud**		
2.1.1.1	Audit iCloud Passwords & Keychain (Manual)	☐	☐
2.1.1.2	Audit iCloud Drive (Manual)	☐	☐
2.1.1.3	Ensure iCloud Drive Document and Desktop Sync Is Disabled (Automated)	☐	☐
2.1.1.4	Audit Security Keys Used With Apple Accounts (Manual)	☐	☐
2.1.1.5	Audit Freeform Sync to iCloud (Manual)	☐	☐
2.1.1.6	Audit Find My Mac (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.2	Audit App Store Password Settings (Manual)	☐	☐
2.2	**Network**		
2.2.1	Ensure Firewall Is Enabled (Automated)	☐	☐
2.2.2	Ensure Firewall Stealth Mode Is Enabled (Automated)	☐	☐
2.3	**General**		
2.3.1	**AirDrop & Handoff**		
2.3.1.1	Ensure AirDrop Is Disabled When Not Actively Transferring Files (Automated)	☐	☐
2.3.1.2	Ensure AirPlay Receiver Is Disabled (Automated)	☐	☐
2.3.2	**Date & Time**		
2.3.2.1	Ensure Set Time and Date Automatically Is Enabled (Automated)	☐	☐
2.3.2.2	Ensure the Time Service Is Enabled (Automated)	☐	☐
2.3.3	**Sharing**		
2.3.3.1	Ensure Screen Sharing Is Disabled (Automated)	☐	☐
2.3.3.2	Ensure File Sharing Is Disabled (Automated)	☐	☐
2.3.3.3	Ensure Printer Sharing Is Disabled (Automated)	☐	☐
2.3.3.4	Ensure Remote Login Is Disabled (Automated)	☐	☐
2.3.3.5	Ensure Remote Management Is Disabled (Automated)	☐	☐
2.3.3.6	Ensure Remote Apple Events Is Disabled (Automated)	☐	☐
2.3.3.7	Ensure Internet Sharing Is Disabled (Automated)	☐	☐
2.3.3.8	Ensure Content Caching Is Disabled (Automated)	☐	☐
2.3.3.9	Ensure Media Sharing Is Disabled (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.3.10	Ensure Bluetooth Sharing Is Disabled (Automated)	☐	☐
2.3.3.11	Ensure Computer Name Does Not Contain PII or Protected Organizational Information (Manual)	☐	☐
2.3.4	**Time Machine**		
2.3.4.1	Ensure Backup Automatically is Enabled If Time Machine Is Enabled (Automated)	☐	☐
2.3.4.2	Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled (Automated)	☐	☐
2.3.5	**Menu Bar**		
2.4	Audit Menu Bar and Control Center Icons (Manual)		
2.4.1	**Apple Intelligence & Siri**	☐	☐
2.5	**Apple Intelligence**		
2.5.1	Ensure External Intelligence Extensions Is Disabled (Automated)		
2.5.1.1	Ensure Writing Tools Is Disabled (Automated)	☐	☐
2.5.1.2	Ensure Mail Summarization Is Disabled (Automated)	☐	☐
2.5.1.3	Ensure Notes Summarization Is Disabled (Automated)	☐	☐
2.5.1.4	**Siri**	☐	☐
2.5.2	Ensure Siri Is Disabled (Automated)		
2.5.2.1	Ensure Listen for (Siri) Is Disabled (Manual)	☐	☐
2.5.2.2	**Privacy & Security**	☐	☐
2.6	**Location Services**		
2.6.1	Ensure Location Services Is Enabled (Automated)		

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.6.1.1	Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled (Automated)	☐	☐
2.6.1.2	Audit Location Services Access (Manual)	☐	☐
2.6.1.3	**Full Disk Access**	☐	☐
2.6.2	Audit Full Disk Access for Applications (Manual)		
2.6.2.1	**Analytics & Improvements**	☐	☐
2.6.3	Ensure Share Mac Analytics Is Disabled (Automated)		
2.6.3.1	Ensure Improve Siri & Dictation Is Disabled (Automated)	☐	☐
2.6.3.2	Ensure Improve Assistive Voice Features Is Disabled (Automated)	☐	☐
2.6.3.3	Ensure 'Share with app developers' Is Disabled (Automated)	☐	☐
2.6.3.4	Ensure Share iCloud Analytics Is Disabled (Manual)	☐	☐
2.6.3.5	Ensure Limit Ad Tracking Is Enabled (Automated)	☐	☐
2.6.4	Ensure Gatekeeper Is Enabled (Automated)	☐	☐
2.6.5	Ensure FileVault Is Enabled (Automated)	☐	☐
2.6.6	Audit Lockdown Mode (Manual)	☐	☐
2.6.7	Ensure an Administrator Password Is Required to Access System-Wide Preferences (Automated)	☐	☐
2.6.8	**Desktop & Dock**	☐	☐
2.7	Ensure Screen Saver Corners Are Secure (Automated)		
2.7.1	Audit iPhone Mirroring (Manual)	☐	☐
2.7.2	**Displays**	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.8	Audit Universal Control Settings (Manual)		
2.8.1	**Spotlight**	☐	☐
2.9	Ensure Help Apple Improve Search Is Disabled (Automated)		
2.9.1	**Battery (Energy Saver)**	☐	☐
2.10	**OS Resuming From Sleep**		
2.10.1	Ensure the OS Is Not Active When Resuming from Standby (Intel) (Manual)		
2.10.1.1	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices (Automated)	☐	☐
2.10.1.2	Ensure Power Nap Is Disabled for Intel Macs (Automated)	☐	☐
2.10.2	Ensure Wake for Network Access Is Disabled (Automated)	☐	☐
2.10.3	**Lock Screen**	☐	☐
2.11	Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled (Automated)		
2.11.1	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately (Automated)	☐	☐
2.11.2	Ensure a Custom Message for the Login Screen Is Enabled (Automated)	☐	☐
2.11.3	Ensure Login Window Displays as Name and Password Is Enabled (Automated)	☐	☐
2.11.4	Ensure Show Password Hints Is Disabled (Automated)	☐	☐
2.11.5	**Touch ID & Password (Login Password)**	☐	☐
2.12	Ensure Users' Accounts Do Not Have a Password Hint (Automated)		

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.12.1	Audit Touch ID (Manual)	☐	☐
2.12.2	**Users & Groups**	☐	☐
2.13	Ensure Guest Account Is Disabled (Automated)		
2.13.1	Ensure Guest Access to Shared Folders Is Disabled (Automated)	☐	☐
2.13.2	Ensure Automatic Login Is Disabled (Automated)	☐	☐
2.13.3	**Game Center**	☐	☐
2.14	Audit Game Center Settings (Manual)		
2.14.1	**Notifications**	☐	☐
2.15	Audit Notification Settings (Manual)		
2.15.1	**Wallet & Apple Pay**	☐	☐
2.16	Audit Wallet & Apple Pay Settings (Manual)		
2.16.1	**Internet Accounts**	☐	☐
2.17	Audit Internet Accounts for Authorized Use (Manual)		
2.17.1	**Keyboard**	☐	☐
2.18	Ensure On-Device Dictation Is Enabled (Automated)		
2.18.1	**Logging and Auditing**	☐	☐
3	Ensure Security Auditing Is Enabled (Automated)		
3.1	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements (Automated)	☐	☐
3.2	Ensure install.log Is Retained for 365 or More Days and No Maximum Size (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.3	Ensure Security Auditing Retention Is Enabled (Automated)	☐	☐
3.4	Ensure Access to Audit Records Is Controlled (Automated)	☐	☐
3.5	Audit Software Inventory (Manual)	☐	☐
3.6	**Network Configurations**	☐	☐
4	Ensure Bonjour Advertising Services Is Disabled (Automated)		
4.1	Ensure HTTP Server Is Disabled (Automated)	☐	☐
4.2	Ensure NFS Server Is Disabled (Automated)	☐	☐
4.3	**System Access, Authentication and Authorization**	☐	☐
5	**File System Permissions and Access Controls**		
5.1	Ensure Home Folders Are Secure (Automated)		
5.1.1	Ensure System Integrity Protection Status (SIP) Is Enabled (Automated)	☐	☐
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled (Automated)	☐	☐
5.1.3	Ensure Signed System Volume (SSV) Is Enabled (Automated)	☐	☐
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated)	☐	☐
5.1.5	Ensure No World Writable Folders Exist in the System Folder (Automated)	☐	☐
5.1.6	Ensure No World Writable Folders Exist in the Library Folder (Automated)	☐	☐
5.1.7	**Account and Password Policy Management**	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2	Ensure Password Account Lockout Threshold Is Configured (Automated)		
5.2.1	Ensure Password Minimum Length Is Configured (Automated)	☐	☐
5.2.2	Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Manual)	☐	☐
5.2.3	Ensure Complex Password Must Contain Numeric Character Is Configured (Manual)	☐	☐
5.2.4	Ensure Complex Password Must Contain Special Character Is Configured (Manual)	☐	☐
5.2.5	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Manual)	☐	☐
5.2.6	Ensure Password Age Is Configured (Automated)	☐	☐
5.2.7	Ensure Password History Is Set to at least 24 (Automated)	☐	☐
5.2.8	**Encryption**	☐	☐
5.3	Ensure all user storage APFS volumes are encrypted (Manual)		
5.3.1	Ensure all user storage CoreStorage volumes are encrypted (Manual)	☐	☐
5.3.2	Ensure the Sudo Timeout Period Is Set to Zero (Automated)	☐	☐
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated)	☐	☐
5.5	Ensure the "root" Account Is Disabled (Automated)	☐	☐
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session (Automated)	☐	☐
5.7	Ensure a Login Window Banner Exists (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.8	Ensure the Guest Home Folder Does Not Exist (Automated)	☐	☐
5.9	Ensure XProtect Is Running and Updated (Automated)	☐	☐
5.10	Ensure Logging Is Enabled for Sudo (Automated)	☐	☐
5.11	**Applications**	☐	☐
6	**Finder**		
6.1	Audit Show All Filename Extensions (Manual)		
6.1.1	**Mail**	☐	☐
6.2	Ensure Protect Mail Activity in Mail Is Enabled (Manual)		
6.2.1	**Safari**	☐	☐
6.3	Ensure Automatic Opening of Safe Files in Safari Is Disabled (Automated)		
6.3.1	Audit History and Remove History Items (Manual)	☐	☐
6.3.2	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled (Automated)	☐	☐
6.3.3	Ensure Prevent Cross-site Tracking in Safari Is Enabled (Automated)	☐	☐
6.3.4	Audit Hide IP Address in Safari Setting (Manual)	☐	☐
6.3.5	Ensure Advertising Privacy Protection in Safari Is Enabled (Automated)	☐	☐
6.3.6	Ensure Show Full Website Address in Safari Is Enabled (Automated)	☐	☐
6.3.7	Audit AutoFill (Manual)	☐	☐
6.3.8	Audit Pop-up Windows (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.3.9	Ensure Show Status Bar Is Enabled (Automated)	☐	☐
6.3.10	**Terminal**	☐	☐
6.4	Ensure Secure Keyboard Entry Terminal.app Is Enabled (Automated)		
6.4.1	**Passwords**	☐	☐
6.5	Audit Passwords (Manual)		
6.5.1	**Supplemental**	☐	☐
7	**CIS Apple macOS Benchmark development collaboration with mSCP**		
7.1	**Apple Push Notification Service (APNs)**		
7.2	**Mobile Configuration Profiles**		
7.3	**Mobile Device Management (MDM) Software**		
7.4			

Internal Only - General

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure Apple-provided Software Updates Are Installed	☐	☐
1.2	Ensure Download New Updates When Available Is Enabled	☐	☐
1.3	Ensure Install of macOS Updates Is Enabled	☐	☐
1.4	Ensure Install Application Updates from the App Store Is Enabled	☐	☐
1.5	Ensure Install Security Responses and System Files Is Enabled	☐	☐
1.6	Ensure Software Update Deferment Is Less Than or Equal to 30 Days	☐	☐
2.1.1.1	Audit iCloud Passwords & Keychain	☐	☐
2.1.1.2	Audit iCloud Drive	☐	☐
2.1.1.3	Ensure iCloud Drive Document and Desktop Sync Is Disabled	☐	☐
2.1.1.5	Audit Freeform Sync to iCloud	☐	☐
2.1.1.6	Audit Find My Mac	☐	☐
2.1.2	Audit App Store Password Settings	☐	☐
2.2.1	Ensure Firewall Is Enabled	☐	☐
2.2.2	Ensure Firewall Stealth Mode Is Enabled	☐	☐
2.3.1.1	Ensure AirDrop Is Disabled When Not Actively Transferring Files	☐	☐
2.3.1.2	Ensure AirPlay Receiver Is Disabled	☐	☐
2.3.3.1	Ensure Screen Sharing Is Disabled	☐	☐
2.3.3.2	Ensure File Sharing Is Disabled	☐	☐
2.3.3.3	Ensure Printer Sharing Is Disabled	☐	☐
2.3.3.4	Ensure Remote Login Is Disabled	☐	☐
2.3.3.5	Ensure Remote Management Is Disabled	☐	☐
2.3.3.6	Ensure Remote Apple Events Is Disabled	☐	☐
2.3.3.7	Ensure Internet Sharing Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.3.3.9	Ensure Media Sharing Is Disabled	☐	☐
2.3.3.10	Ensure Bluetooth Sharing Is Disabled	☐	☐
2.3.4.1	Ensure Backup Automatically is Enabled If Time Machine Is Enabled	☐	☐
2.3.4.2	Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled	☐	☐
2.5.1.1	Ensure External Intelligence Extensions Is Disabled	☐	☐
2.5.1.2	Ensure Writing Tools Is Disabled	☐	☐
2.5.1.3	Ensure Mail Summarization Is Disabled	☐	☐
2.5.1.4	Ensure Notes Summarization Is Disabled	☐	☐
2.5.2.1	Ensure Siri Is Disabled	☐	☐
2.5.2.2	Ensure Listen for (Siri) Is Disabled	☐	☐
2.6.1.1	Ensure Location Services Is Enabled	☐	☐
2.6.1.2	Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled	☐	☐
2.6.1.3	Audit Location Services Access	☐	☐
2.6.2.1	Audit Full Disk Access for Applications	☐	☐
2.6.3.1	Ensure Share Mac Analytics Is Disabled	☐	☐
2.6.3.2	Ensure Improve Siri & Dictation Is Disabled	☐	☐
2.6.3.3	Ensure Improve Assistive Voice Features Is Disabled	☐	☐
2.6.3.4	Ensure 'Share with app developers' Is Disabled	☐	☐
2.6.3.5	Ensure Share iCloud Analytics Is Disabled	☐	☐
2.6.5	Ensure Gatekeeper Is Enabled	☐	☐
2.6.6	Ensure FileVault Is Enabled	☐	☐
2.6.8	Ensure an Administrator Password Is Required to Access System-Wide Preferences	☐	☐
2.7.1	Ensure Screen Saver Corners Are Secure	☐	☐
2.8.1	Audit Universal Control Settings	☐	☐
2.10.1.1	Ensure the OS Is Not Active When Resuming from Standby (Intel)	☐	☐
2.10.1.2	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	☐	☐
2.10.2	Ensure Power Nap Is Disabled for Intel Macs	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.11.1	Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled	☐	☐
2.11.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	☐	☐
2.11.3	Ensure a Custom Message for the Login Screen Is Enabled	☐	☐
2.11.4	Ensure Login Window Displays as Name and Password Is Enabled	☐	☐
2.11.5	Ensure Show Password Hints Is Disabled	☐	☐
2.12.2	Audit Touch ID	☐	☐
2.13.2	Ensure Guest Access to Shared Folders Is Disabled	☐	☐
2.13.3	Ensure Automatic Login Is Disabled	☐	☐
2.15.1	Audit Notification Settings	☐	☐
2.17.1	Audit Internet Accounts for Authorized Use	☐	☐
2.18.1	Ensure On-Device Dictation Is Enabled	☐	☐
3.1	Ensure Security Auditing Is Enabled	☐	☐
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	☐	☐
3.5	Ensure Access to Audit Records Is Controlled	☐	☐
3.6	Audit Software Inventory	☐	☐
4.1	Ensure Bonjour Advertising Services Is Disabled	☐	☐
4.2	Ensure HTTP Server Is Disabled	☐	☐
4.3	Ensure NFS Server Is Disabled	☐	☐
5.1.1	Ensure Home Folders Are Secure	☐	☐
5.1.2	Ensure System Integrity Protection Status (SIP) Is Enabled	☐	☐
5.1.3	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	☐	☐
5.1.4	Ensure Signed System Volume (SSV) Is Enabled	☐	☐
5.1.5	Ensure Appropriate Permissions Are Enabled for System Wide Applications	☐	☐
5.1.6	Ensure No World Writable Folders Exist in the System Folder	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.1.7	Ensure No World Writable Folders Exist in the Library Folder	☐	☐
5.2.7	Ensure Password Age Is Configured	☐	☐
5.3.1	Ensure all user storage APFS volumes are encrypted	☐	☐
5.3.2	Ensure all user storage CoreStorage volumes are encrypted	☐	☐
5.4	Ensure the Sudo Timeout Period Is Set to Zero	☐	☐
5.5	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	☐	☐
5.6	Ensure the "root" Account Is Disabled	☐	☐
5.7	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	☐	☐
5.8	Ensure a Login Window Banner Exists	☐	☐
5.9	Ensure the Guest Home Folder Does Not Exist	☐	☐
5.10	Ensure XProtect Is Running and Updated	☐	☐
5.11	Ensure Logging Is Enabled for Sudo	☐	☐
6.1.1	Audit Show All Filename Extensions	☐	☐
6.2.1	Ensure Protect Mail Activity in Mail Is Enabled	☐	☐
6.3.1	Ensure Automatic Opening of Safe Files in Safari Is Disabled	☐	☐
6.3.2	Audit History and Remove History Items	☐	☐
6.3.3	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	☐	☐
6.3.4	Ensure Prevent Cross-site Tracking in Safari Is Enabled	☐	☐
6.3.5	Audit Hide IP Address in Safari Setting	☐	☐
6.3.6	Ensure Advertising Privacy Protection in Safari Is Enabled	☐	☐
6.3.7	Ensure Show Full Website Address in Safari Is Enabled	☐	☐
6.3.8	Audit AutoFill	☐	☐
6.3.9	Audit Pop-up Windows	☐	☐
6.3.10	Ensure Show Status Bar Is Enabled	☐	☐
6.4.1	Ensure Secure Keyboard Entry Terminal.app Is Enabled	☐	☐

Internal Only - General

Internal Only - General

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure Apple-provided Software Updates Are Installed	☐	☐
1.2	Ensure Download New Updates When Available Is Enabled	☐	☐
1.3	Ensure Install of macOS Updates Is Enabled	☐	☐
1.4	Ensure Install Application Updates from the App Store Is Enabled	☐	☐
1.5	Ensure Install Security Responses and System Files Is Enabled	☐	☐
1.6	Ensure Software Update Deferment Is Less Than or Equal to 30 Days	☐	☐
2.1.1.1	Audit iCloud Passwords & Keychain	☐	☐
2.1.1.2	Audit iCloud Drive	☐	☐
2.1.1.3	Ensure iCloud Drive Document and Desktop Sync Is Disabled	☐	☐
2.1.1.4	Audit Security Keys Used With Apple Accounts	☐	☐
2.1.1.5	Audit Freeform Sync to iCloud	☐	☐
2.1.1.6	Audit Find My Mac	☐	☐
2.1.2	Audit App Store Password Settings	☐	☐
2.2.1	Ensure Firewall Is Enabled	☐	☐
2.2.2	Ensure Firewall Stealth Mode Is Enabled	☐	☐
2.3.1.1	Ensure AirDrop Is Disabled When Not Actively Transferring Files	☐	☐
2.3.1.2	Ensure AirPlay Receiver Is Disabled	☐	☐
2.3.2.1	Ensure Set Time and Date Automatically Is Enabled	☐	☐
2.3.2.2	Ensure the Time Service Is Enabled	☐	☐
2.3.3.1	Ensure Screen Sharing Is Disabled	☐	☐
2.3.3.2	Ensure File Sharing Is Disabled	☐	☐
2.3.3.3	Ensure Printer Sharing Is Disabled	☐	☐
2.3.3.4	Ensure Remote Login Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.3.3.5	Ensure Remote Management Is Disabled	☐	☐
2.3.3.6	Ensure Remote Apple Events Is Disabled	☐	☐
2.3.3.7	Ensure Internet Sharing Is Disabled	☐	☐
2.3.3.8	Ensure Content Caching Is Disabled	☐	☐
2.3.3.9	Ensure Media Sharing Is Disabled	☐	☐
2.3.3.10	Ensure Bluetooth Sharing Is Disabled	☐	☐
2.3.3.11	Ensure Computer Name Does Not Contain PII or Protected Organizational Information	☐	☐
2.3.4.1	Ensure Backup Automatically is Enabled If Time Machine Is Enabled	☐	☐
2.3.4.2	Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled	☐	☐
2.5.1.1	Ensure External Intelligence Extensions Is Disabled	☐	☐
2.5.1.2	Ensure Writing Tools Is Disabled	☐	☐
2.5.1.3	Ensure Mail Summarization Is Disabled	☐	☐
2.5.1.4	Ensure Notes Summarization Is Disabled	☐	☐
2.5.2.1	Ensure Siri Is Disabled	☐	☐
2.5.2.2	Ensure Listen for (Siri) Is Disabled	☐	☐
2.6.1.1	Ensure Location Services Is Enabled	☐	☐
2.6.1.2	Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled	☐	☐
2.6.1.3	Audit Location Services Access	☐	☐
2.6.2.1	Audit Full Disk Access for Applications	☐	☐
2.6.3.1	Ensure Share Mac Analytics Is Disabled	☐	☐
2.6.3.2	Ensure Improve Siri & Dictation Is Disabled	☐	☐
2.6.3.3	Ensure Improve Assistive Voice Features Is Disabled	☐	☐
2.6.3.4	Ensure 'Share with app developers' Is Disabled	☐	☐
2.6.3.5	Ensure Share iCloud Analytics Is Disabled	☐	☐
2.6.4	Ensure Limit Ad Tracking Is Enabled	☐	☐
2.6.5	Ensure Gatekeeper Is Enabled	☐	☐
2.6.6	Ensure FileVault Is Enabled	☐	☐
2.6.7	Audit Lockdown Mode	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.6.8	Ensure an Administrator Password Is Required to Access System-Wide Preferences	☐	☐
2.7.1	Ensure Screen Saver Corners Are Secure	☐	☐
2.8.1	Audit Universal Control Settings	☐	☐
2.10.1.1	Ensure the OS Is Not Active When Resuming from Standby (Intel)	☐	☐
2.10.1.2	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	☐	☐
2.10.2	Ensure Power Nap Is Disabled for Intel Macs	☐	☐
2.10.3	Ensure Wake for Network Access Is Disabled	☐	☐
2.11.1	Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled	☐	☐
2.11.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	☐	☐
2.11.3	Ensure a Custom Message for the Login Screen Is Enabled	☐	☐
2.11.4	Ensure Login Window Displays as Name and Password Is Enabled	☐	☐
2.11.5	Ensure Show Password Hints Is Disabled	☐	☐
2.12.1	Ensure Users' Accounts Do Not Have a Password Hint	☐	☐
2.12.2	Audit Touch ID	☐	☐
2.13.1	Ensure Guest Account Is Disabled	☐	☐
2.13.2	Ensure Guest Access to Shared Folders Is Disabled	☐	☐
2.13.3	Ensure Automatic Login Is Disabled	☐	☐
2.15.1	Audit Notification Settings	☐	☐
2.17.1	Audit Internet Accounts for Authorized Use	☐	☐
2.18.1	Ensure On-Device Dictation Is Enabled	☐	☐
3.1	Ensure Security Auditing Is Enabled	☐	☐
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	☐	☐
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.4	Ensure Security Auditing Retention Is Enabled	☐	☐
3.5	Ensure Access to Audit Records Is Controlled	☐	☐
3.6	Audit Software Inventory	☐	☐
4.1	Ensure Bonjour Advertising Services Is Disabled	☐	☐
4.2	Ensure HTTP Server Is Disabled	☐	☐
4.3	Ensure NFS Server Is Disabled	☐	☐
5.1.1	Ensure Home Folders Are Secure	☐	☐
5.1.2	Ensure System Integrity Protection Status (SIP) Is Enabled	☐	☐
5.1.3	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	☐	☐
5.1.4	Ensure Signed System Volume (SSV) Is Enabled	☐	☐
5.1.5	Ensure Appropriate Permissions Are Enabled for System Wide Applications	☐	☐
5.1.6	Ensure No World Writable Folders Exist in the System Folder	☐	☐
5.1.7	Ensure No World Writable Folders Exist in the Library Folder	☐	☐
5.2.1	Ensure Password Account Lockout Threshold Is Configured	☐	☐
5.2.2	Ensure Password Minimum Length Is Configured	☐	☐
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	☐	☐
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	☐	☐
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	☐	☐
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	☐	☐
5.2.7	Ensure Password Age Is Configured	☐	☐
5.2.8	Ensure Password History Is Set to at least 24	☐	☐
5.3.1	Ensure all user storage APFS volumes are encrypted	☐	☐
5.3.2	Ensure all user storage CoreStorage volumes are encrypted	☐	☐
5.4	Ensure the Sudo Timeout Period Is Set to Zero	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.5	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	☐	☐
5.6	Ensure the "root" Account Is Disabled	☐	☐
5.7	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	☐	☐
5.8	Ensure a Login Window Banner Exists	☐	☐
5.9	Ensure the Guest Home Folder Does Not Exist	☐	☐
5.10	Ensure XProtect Is Running and Updated	☐	☐
5.11	Ensure Logging Is Enabled for Sudo	☐	☐
6.1.1	Audit Show All Filename Extensions	☐	☐
6.2.1	Ensure Protect Mail Activity in Mail Is Enabled	☐	☐
6.3.1	Ensure Automatic Opening of Safe Files in Safari Is Disabled	☐	☐
6.3.2	Audit History and Remove History Items	☐	☐
6.3.3	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	☐	☐
6.3.4	Ensure Prevent Cross-site Tracking in Safari Is Enabled	☐	☐
6.3.5	Audit Hide IP Address in Safari Setting	☐	☐
6.3.6	Ensure Advertising Privacy Protection in Safari Is Enabled	☐	☐
6.3.7	Ensure Show Full Website Address in Safari Is Enabled	☐	☐
6.3.8	Audit AutoFill	☐	☐
6.3.9	Audit Pop-up Windows	☐	☐
6.3.10	Ensure Show Status Bar Is Enabled	☐	☐
6.4.1	Ensure Secure Keyboard Entry Terminal.app Is Enabled	☐	☐
6.5.1	Audit Passwords	☐	☐

Internal Only - General

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure Apple-provided Software Updates Are Installed	☐	☐
1.2	Ensure Download New Updates When Available Is Enabled	☐	☐
1.3	Ensure Install of macOS Updates Is Enabled	☐	☐
1.4	Ensure Install Application Updates from the App Store Is Enabled	☐	☐
1.5	Ensure Install Security Responses and System Files Is Enabled	☐	☐
1.6	Ensure Software Update Deferment Is Less Than or Equal to 30 Days	☐	☐
2.1.1.1	Audit iCloud Passwords & Keychain	☐	☐
2.1.1.2	Audit iCloud Drive	☐	☐
2.1.1.3	Ensure iCloud Drive Document and Desktop Sync Is Disabled	☐	☐
2.1.1.4	Audit Security Keys Used With Apple Accounts	☐	☐
2.1.1.5	Audit Freeform Sync to iCloud	☐	☐
2.1.1.6	Audit Find My Mac	☐	☐
2.1.2	Audit App Store Password Settings	☐	☐
2.2.1	Ensure Firewall Is Enabled	☐	☐
2.2.2	Ensure Firewall Stealth Mode Is Enabled	☐	☐
2.3.1.1	Ensure AirDrop Is Disabled When Not Actively Transferring Files	☐	☐
2.3.1.2	Ensure AirPlay Receiver Is Disabled	☐	☐
2.3.2.1	Ensure Set Time and Date Automatically Is Enabled	☐	☐
2.3.2.2	Ensure the Time Service Is Enabled	☐	☐
2.3.3.1	Ensure Screen Sharing Is Disabled	☐	☐
2.3.3.2	Ensure File Sharing Is Disabled	☐	☐
2.3.3.3	Ensure Printer Sharing Is Disabled	☐	☐
2.3.3.4	Ensure Remote Login Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.3.3.5	Ensure Remote Management Is Disabled	☐	☐
2.3.3.6	Ensure Remote Apple Events Is Disabled	☐	☐
2.3.3.7	Ensure Internet Sharing Is Disabled	☐	☐
2.3.3.8	Ensure Content Caching Is Disabled	☐	☐
2.3.3.9	Ensure Media Sharing Is Disabled	☐	☐
2.3.3.10	Ensure Bluetooth Sharing Is Disabled	☐	☐
2.3.3.11	Ensure Computer Name Does Not Contain PII or Protected Organizational Information	☐	☐
2.3.4.1	Ensure Backup Automatically is Enabled If Time Machine Is Enabled	☐	☐
2.3.4.2	Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled	☐	☐
2.4.1	Audit Menu Bar and Control Center Icons	☐	☐
2.5.1.1	Ensure External Intelligence Extensions Is Disabled	☐	☐
2.5.1.2	Ensure Writing Tools Is Disabled	☐	☐
2.5.1.3	Ensure Mail Summarization Is Disabled	☐	☐
2.5.1.4	Ensure Notes Summarization Is Disabled	☐	☐
2.5.2.1	Ensure Siri Is Disabled	☐	☐
2.5.2.2	Ensure Listen for (Siri) Is Disabled	☐	☐
2.6.1.1	Ensure Location Services Is Enabled	☐	☐
2.6.1.2	Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled	☐	☐
2.6.1.3	Audit Location Services Access	☐	☐
2.6.2.1	Audit Full Disk Access for Applications	☐	☐
2.6.3.1	Ensure Share Mac Analytics Is Disabled	☐	☐
2.6.3.2	Ensure Improve Siri & Dictation Is Disabled	☐	☐
2.6.3.3	Ensure Improve Assistive Voice Features Is Disabled	☐	☐
2.6.3.4	Ensure 'Share with app developers' Is Disabled	☐	☐
2.6.3.5	Ensure Share iCloud Analytics Is Disabled	☐	☐
2.6.4	Ensure Limit Ad Tracking Is Enabled	☐	☐
2.6.5	Ensure Gatekeeper Is Enabled	☐	☐
2.6.6	Ensure FileVault Is Enabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.6.7	Audit Lockdown Mode	☐	☐
2.6.8	Ensure an Administrator Password Is Required to Access System-Wide Preferences	☐	☐
2.7.1	Ensure Screen Saver Corners Are Secure	☐	☐
2.8.1	Audit Universal Control Settings	☐	☐
2.10.1.1	Ensure the OS Is Not Active When Resuming from Standby (Intel)	☐	☐
2.10.1.2	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	☐	☐
2.10.2	Ensure Power Nap Is Disabled for Intel Macs	☐	☐
2.10.3	Ensure Wake for Network Access Is Disabled	☐	☐
2.11.1	Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled	☐	☐
2.11.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	☐	☐
2.11.3	Ensure a Custom Message for the Login Screen Is Enabled	☐	☐
2.11.4	Ensure Login Window Displays as Name and Password Is Enabled	☐	☐
2.11.5	Ensure Show Password Hints Is Disabled	☐	☐
2.12.1	Ensure Users' Accounts Do Not Have a Password Hint	☐	☐
2.12.2	Audit Touch ID	☐	☐
2.13.1	Ensure Guest Account Is Disabled	☐	☐
2.13.2	Ensure Guest Access to Shared Folders Is Disabled	☐	☐
2.13.3	Ensure Automatic Login Is Disabled	☐	☐
2.15.1	Audit Notification Settings	☐	☐
2.17.1	Audit Internet Accounts for Authorized Use	☐	☐
2.18.1	Ensure On-Device Dictation Is Enabled	☐	☐
3.1	Ensure Security Auditing Is Enabled	☐	☐
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	☐	☐
3.4	Ensure Security Auditing Retention Is Enabled	☐	☐
3.5	Ensure Access to Audit Records Is Controlled	☐	☐
3.6	Audit Software Inventory	☐	☐
4.1	Ensure Bonjour Advertising Services Is Disabled	☐	☐
4.2	Ensure HTTP Server Is Disabled	☐	☐
4.3	Ensure NFS Server Is Disabled	☐	☐
5.1.1	Ensure Home Folders Are Secure	☐	☐
5.1.2	Ensure System Integrity Protection Status (SIP) Is Enabled	☐	☐
5.1.3	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	☐	☐
5.1.4	Ensure Signed System Volume (SSV) Is Enabled	☐	☐
5.1.5	Ensure Appropriate Permissions Are Enabled for System Wide Applications	☐	☐
5.1.6	Ensure No World Writable Folders Exist in the System Folder	☐	☐
5.1.7	Ensure No World Writable Folders Exist in the Library Folder	☐	☐
5.2.1	Ensure Password Account Lockout Threshold Is Configured	☐	☐
5.2.2	Ensure Password Minimum Length Is Configured	☐	☐
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	☐	☐
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	☐	☐
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	☐	☐
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	☐	☐
5.2.7	Ensure Password Age Is Configured	☐	☐
5.2.8	Ensure Password History Is Set to at least 24	☐	☐
5.3.1	Ensure all user storage APFS volumes are encrypted	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.3.2	Ensure all user storage CoreStorage volumes are encrypted	☐	☐
5.4	Ensure the Sudo Timeout Period Is Set to Zero	☐	☐
5.5	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	☐	☐
5.6	Ensure the "root" Account Is Disabled	☐	☐
5.7	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	☐	☐
5.8	Ensure a Login Window Banner Exists	☐	☐
5.9	Ensure the Guest Home Folder Does Not Exist	☐	☐
5.10	Ensure XProtect Is Running and Updated	☐	☐
5.11	Ensure Logging Is Enabled for Sudo	☐	☐
6.1.1	Audit Show All Filename Extensions	☐	☐
6.2.1	Ensure Protect Mail Activity in Mail Is Enabled	☐	☐
6.3.1	Ensure Automatic Opening of Safe Files in Safari Is Disabled	☐	☐
6.3.2	Audit History and Remove History Items	☐	☐
6.3.3	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	☐	☐
6.3.4	Ensure Prevent Cross-site Tracking in Safari Is Enabled	☐	☐
6.3.5	Audit Hide IP Address in Safari Setting	☐	☐
6.3.6	Ensure Advertising Privacy Protection in Safari Is Enabled	☐	☐
6.3.7	Ensure Show Full Website Address in Safari Is Enabled	☐	☐
6.3.8	Audit AutoFill	☐	☐
6.3.9	Audit Pop-up Windows	☐	☐
6.3.10	Ensure Show Status Bar Is Enabled	☐	☐
6.4.1	Ensure Secure Keyboard Entry Terminal.app Is Enabled	☐	☐
6.5.1	Audit Passwords	☐	☐

Internal Only - General

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.9.1	Ensure Help Apple Improve Search Is Disabled	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure Apple-provided Software Updates Are Installed	☐	☐
1.2	Ensure Download New Updates When Available Is Enabled	☐	☐
1.3	Ensure Install of macOS Updates Is Enabled	☐	☐
1.4	Ensure Install Application Updates from the App Store Is Enabled	☐	☐
1.5	Ensure Install Security Responses and System Files Is Enabled	☐	☐
1.6	Ensure Software Update Deferment Is Less Than or Equal to 30 Days	☐	☐
2.1.1.1	Audit iCloud Passwords & Keychain	☐	☐
2.1.1.2	Audit iCloud Drive	☐	☐
2.1.1.3	Ensure iCloud Drive Document and Desktop Sync Is Disabled	☐	☐
2.1.1.4	Audit Security Keys Used With Apple Accounts	☐	☐
2.1.1.5	Audit Freeform Sync to iCloud	☐	☐
2.1.1.6	Audit Find My Mac	☐	☐
2.1.2	Audit App Store Password Settings	☐	☐
2.2.1	Ensure Firewall Is Enabled	☐	☐
2.2.2	Ensure Firewall Stealth Mode Is Enabled	☐	☐
2.3.1.1	Ensure AirDrop Is Disabled When Not Actively Transferring Files	☐	☐
2.3.1.2	Ensure AirPlay Receiver Is Disabled	☐	☐
2.3.3.1	Ensure Screen Sharing Is Disabled	☐	☐
2.3.3.2	Ensure File Sharing Is Disabled	☐	☐
2.3.3.3	Ensure Printer Sharing Is Disabled	☐	☐
2.3.3.4	Ensure Remote Login Is Disabled	☐	☐
2.3.3.5	Ensure Remote Management Is Disabled	☐	☐
2.3.3.6	Ensure Remote Apple Events Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.3.3.7	Ensure Internet Sharing Is Disabled	☐	☐
2.3.3.9	Ensure Media Sharing Is Disabled	☐	☐
2.3.3.10	Ensure Bluetooth Sharing Is Disabled	☐	☐
2.3.3.11	Ensure Computer Name Does Not Contain PII or Protected Organizational Information	☐	☐
2.3.4.1	Ensure Backup Automatically is Enabled If Time Machine Is Enabled	☐	☐
2.3.4.2	Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled	☐	☐
2.5.1.1	Ensure External Intelligence Extensions Is Disabled	☐	☐
2.5.1.2	Ensure Writing Tools Is Disabled	☐	☐
2.5.1.3	Ensure Mail Summarization Is Disabled	☐	☐
2.5.1.4	Ensure Notes Summarization Is Disabled	☐	☐
2.5.2.1	Ensure Siri Is Disabled	☐	☐
2.5.2.2	Ensure Listen for (Siri) Is Disabled	☐	☐
2.6.1.1	Ensure Location Services Is Enabled	☐	☐
2.6.1.2	Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled	☐	☐
2.6.1.3	Audit Location Services Access	☐	☐
2.6.2.1	Audit Full Disk Access for Applications	☐	☐
2.6.3.1	Ensure Share Mac Analytics Is Disabled	☐	☐
2.6.3.2	Ensure Improve Siri & Dictation Is Disabled	☐	☐
2.6.3.3	Ensure Improve Assistive Voice Features Is Disabled	☐	☐
2.6.3.4	Ensure 'Share with app developers' Is Disabled	☐	☐
2.6.3.5	Ensure Share iCloud Analytics Is Disabled	☐	☐
2.6.5	Ensure Gatekeeper Is Enabled	☐	☐
2.6.6	Ensure FileVault Is Enabled	☐	☐
2.6.7	Audit Lockdown Mode	☐	☐
2.6.8	Ensure an Administrator Password Is Required to Access System-Wide Preferences	☐	☐
2.7.1	Ensure Screen Saver Corners Are Secure	☐	☐
2.8.1	Audit Universal Control Settings	☐	☐
2.9.1	Ensure Help Apple Improve Search Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.10.1.1	Ensure the OS Is Not Active When Resuming from Standby (Intel)	☐	☐
2.10.1.2	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	☐	☐
2.10.2	Ensure Power Nap Is Disabled for Intel Macs	☐	☐
2.11.1	Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled	☐	☐
2.11.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	☐	☐
2.11.3	Ensure a Custom Message for the Login Screen Is Enabled	☐	☐
2.11.4	Ensure Login Window Displays as Name and Password Is Enabled	☐	☐
2.11.5	Ensure Show Password Hints Is Disabled	☐	☐
2.12.1	Ensure Users' Accounts Do Not Have a Password Hint	☐	☐
2.12.2	Audit Touch ID	☐	☐
2.13.1	Ensure Guest Account Is Disabled	☐	☐
2.13.2	Ensure Guest Access to Shared Folders Is Disabled	☐	☐
2.13.3	Ensure Automatic Login Is Disabled	☐	☐
2.15.1	Audit Notification Settings	☐	☐
2.17.1	Audit Internet Accounts for Authorized Use	☐	☐
2.18.1	Ensure On-Device Dictation Is Enabled	☐	☐
3.1	Ensure Security Auditing Is Enabled	☐	☐
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	☐	☐
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	☐	☐
3.4	Ensure Security Auditing Retention Is Enabled	☐	☐
3.5	Ensure Access to Audit Records Is Controlled	☐	☐
3.6	Audit Software Inventory	☐	☐
4.1	Ensure Bonjour Advertising Services Is Disabled	☐	☐
4.2	Ensure HTTP Server Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
4.3	Ensure NFS Server Is Disabled	☐	☐
5.1.1	Ensure Home Folders Are Secure	☐	☐
5.1.2	Ensure System Integrity Protection Status (SIP) Is Enabled	☐	☐
5.1.3	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	☐	☐
5.1.4	Ensure Signed System Volume (SSV) Is Enabled	☐	☐
5.1.5	Ensure Appropriate Permissions Are Enabled for System Wide Applications	☐	☐
5.1.6	Ensure No World Writable Folders Exist in the System Folder	☐	☐
5.1.7	Ensure No World Writable Folders Exist in the Library Folder	☐	☐
5.2.1	Ensure Password Account Lockout Threshold Is Configured	☐	☐
5.2.2	Ensure Password Minimum Length Is Configured	☐	☐
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	☐	☐
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	☐	☐
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	☐	☐
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	☐	☐
5.2.7	Ensure Password Age Is Configured	☐	☐
5.2.8	Ensure Password History Is Set to at least 24	☐	☐
5.3.1	Ensure all user storage APFS volumes are encrypted	☐	☐
5.4	Ensure the Sudo Timeout Period Is Set to Zero	☐	☐
5.5	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	☐	☐
5.6	Ensure the "root" Account Is Disabled	☐	☐
5.7	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	☐	☐
5.8	Ensure a Login Window Banner Exists	☐	☐
5.9	Ensure the Guest Home Folder Does Not Exist	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.10	Ensure XProtect Is Running and Updated	☐	☐
5.11	Ensure Logging Is Enabled for Sudo	☐	☐
6.1.1	Audit Show All Filename Extensions	☐	☐
6.2.1	Ensure Protect Mail Activity in Mail Is Enabled	☐	☐
6.3.1	Ensure Automatic Opening of Safe Files in Safari Is Disabled	☐	☐
6.3.2	Audit History and Remove History Items	☐	☐
6.3.3	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	☐	☐
6.3.4	Ensure Prevent Cross-site Tracking in Safari Is Enabled	☐	☐
6.3.5	Audit Hide IP Address in Safari Setting	☐	☐
6.3.6	Ensure Advertising Privacy Protection in Safari Is Enabled	☐	☐
6.3.7	Ensure Show Full Website Address in Safari Is Enabled	☐	☐
6.3.8	Audit AutoFill	☐	☐
6.3.9	Audit Pop-up Windows	☐	☐
6.3.10	Ensure Show Status Bar Is Enabled	☐	☐
6.5.1	Audit Passwords	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure Apple-provided Software Updates Are Installed	☐	☐
1.2	Ensure Download New Updates When Available Is Enabled	☐	☐
1.3	Ensure Install of macOS Updates Is Enabled	☐	☐
1.4	Ensure Install Application Updates from the App Store Is Enabled	☐	☐
1.5	Ensure Install Security Responses and System Files Is Enabled	☐	☐
1.6	Ensure Software Update Deferment Is Less Than or Equal to 30 Days	☐	☐
2.1.1.1	Audit iCloud Passwords & Keychain	☐	☐
2.1.1.2	Audit iCloud Drive	☐	☐
2.1.1.3	Ensure iCloud Drive Document and Desktop Sync Is Disabled	☐	☐
2.1.1.4	Audit Security Keys Used With Apple Accounts	☐	☐
2.1.1.5	Audit Freeform Sync to iCloud	☐	☐
2.1.1.6	Audit Find My Mac	☐	☐
2.1.2	Audit App Store Password Settings	☐	☐
2.2.1	Ensure Firewall Is Enabled	☐	☐
2.2.2	Ensure Firewall Stealth Mode Is Enabled	☐	☐
2.3.1.1	Ensure AirDrop Is Disabled When Not Actively Transferring Files	☐	☐
2.3.1.2	Ensure AirPlay Receiver Is Disabled	☐	☐
2.3.2.1	Ensure Set Time and Date Automatically Is Enabled	☐	☐
2.3.2.2	Ensure the Time Service Is Enabled	☐	☐
2.3.3.1	Ensure Screen Sharing Is Disabled	☐	☐
2.3.3.2	Ensure File Sharing Is Disabled	☐	☐
2.3.3.3	Ensure Printer Sharing Is Disabled	☐	☐
2.3.3.4	Ensure Remote Login Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.3.3.5	Ensure Remote Management Is Disabled	☐	☐
2.3.3.6	Ensure Remote Apple Events Is Disabled	☐	☐
2.3.3.7	Ensure Internet Sharing Is Disabled	☐	☐
2.3.3.8	Ensure Content Caching Is Disabled	☐	☐
2.3.3.9	Ensure Media Sharing Is Disabled	☐	☐
2.3.3.10	Ensure Bluetooth Sharing Is Disabled	☐	☐
2.3.3.11	Ensure Computer Name Does Not Contain PII or Protected Organizational Information	☐	☐
2.3.4.1	Ensure Backup Automatically is Enabled If Time Machine Is Enabled	☐	☐
2.3.4.2	Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled	☐	☐
2.4.1	Audit Menu Bar and Control Center Icons	☐	☐
2.5.1.1	Ensure External Intelligence Extensions Is Disabled	☐	☐
2.5.1.2	Ensure Writing Tools Is Disabled	☐	☐
2.5.1.3	Ensure Mail Summarization Is Disabled	☐	☐
2.5.1.4	Ensure Notes Summarization Is Disabled	☐	☐
2.5.2.1	Ensure Siri Is Disabled	☐	☐
2.5.2.2	Ensure Listen for (Siri) Is Disabled	☐	☐
2.6.1.1	Ensure Location Services Is Enabled	☐	☐
2.6.1.2	Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled	☐	☐
2.6.1.3	Audit Location Services Access	☐	☐
2.6.2.1	Audit Full Disk Access for Applications	☐	☐
2.6.3.1	Ensure Share Mac Analytics Is Disabled	☐	☐
2.6.3.2	Ensure Improve Siri & Dictation Is Disabled	☐	☐
2.6.3.3	Ensure Improve Assistive Voice Features Is Disabled	☐	☐
2.6.3.4	Ensure 'Share with app developers' Is Disabled	☐	☐
2.6.3.5	Ensure Share iCloud Analytics Is Disabled	☐	☐
2.6.4	Ensure Limit Ad Tracking Is Enabled	☐	☐
2.6.5	Ensure Gatekeeper Is Enabled	☐	☐
2.6.6	Ensure FileVault Is Enabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.6.7	Audit Lockdown Mode	☐	☐
2.6.8	Ensure an Administrator Password Is Required to Access System-Wide Preferences	☐	☐
2.7.1	Ensure Screen Saver Corners Are Secure	☐	☐
2.8.1	Audit Universal Control Settings	☐	☐
2.9.1	Ensure Help Apple Improve Search Is Disabled	☐	☐
2.10.1.1	Ensure the OS Is Not Active When Resuming from Standby (Intel)	☐	☐
2.10.1.2	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	☐	☐
2.10.2	Ensure Power Nap Is Disabled for Intel Macs	☐	☐
2.10.3	Ensure Wake for Network Access Is Disabled	☐	☐
2.11.1	Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled	☐	☐
2.11.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	☐	☐
2.11.3	Ensure a Custom Message for the Login Screen Is Enabled	☐	☐
2.11.4	Ensure Login Window Displays as Name and Password Is Enabled	☐	☐
2.11.5	Ensure Show Password Hints Is Disabled	☐	☐
2.12.1	Ensure Users' Accounts Do Not Have a Password Hint	☐	☐
2.12.2	Audit Touch ID	☐	☐
2.13.1	Ensure Guest Account Is Disabled	☐	☐
2.13.2	Ensure Guest Access to Shared Folders Is Disabled	☐	☐
2.13.3	Ensure Automatic Login Is Disabled	☐	☐
2.15.1	Audit Notification Settings	☐	☐
2.17.1	Audit Internet Accounts for Authorized Use	☐	☐
2.18.1	Ensure On-Device Dictation Is Enabled	☐	☐
3.1	Ensure Security Auditing Is Enabled	☐	☐
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	☐	☐
3.4	Ensure Security Auditing Retention Is Enabled	☐	☐
3.5	Ensure Access to Audit Records Is Controlled	☐	☐
3.6	Audit Software Inventory	☐	☐
4.1	Ensure Bonjour Advertising Services Is Disabled	☐	☐
4.2	Ensure HTTP Server Is Disabled	☐	☐
4.3	Ensure NFS Server Is Disabled	☐	☐
5.1.1	Ensure Home Folders Are Secure	☐	☐
5.1.2	Ensure System Integrity Protection Status (SIP) Is Enabled	☐	☐
5.1.3	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	☐	☐
5.1.4	Ensure Signed System Volume (SSV) Is Enabled	☐	☐
5.1.5	Ensure Appropriate Permissions Are Enabled for System Wide Applications	☐	☐
5.1.6	Ensure No World Writable Folders Exist in the System Folder	☐	☐
5.1.7	Ensure No World Writable Folders Exist in the Library Folder	☐	☐
5.2.1	Ensure Password Account Lockout Threshold Is Configured	☐	☐
5.2.2	Ensure Password Minimum Length Is Configured	☐	☐
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	☐	☐
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	☐	☐
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	☐	☐
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	☐	☐
5.2.7	Ensure Password Age Is Configured	☐	☐
5.2.8	Ensure Password History Is Set to at least 24	☐	☐
5.3.1	Ensure all user storage APFS volumes are encrypted	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.3.2	Ensure all user storage CoreStorage volumes are encrypted	☐	☐
5.4	Ensure the Sudo Timeout Period Is Set to Zero	☐	☐
5.5	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	☐	☐
5.6	Ensure the "root" Account Is Disabled	☐	☐
5.7	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	☐	☐
5.8	Ensure a Login Window Banner Exists	☐	☐
5.9	Ensure the Guest Home Folder Does Not Exist	☐	☐
5.10	Ensure XProtect Is Running and Updated	☐	☐
5.11	Ensure Logging Is Enabled for Sudo	☐	☐
6.1.1	Audit Show All Filename Extensions	☐	☐
6.2.1	Ensure Protect Mail Activity in Mail Is Enabled	☐	☐
6.3.1	Ensure Automatic Opening of Safe Files in Safari Is Disabled	☐	☐
6.3.2	Audit History and Remove History Items	☐	☐
6.3.3	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	☐	☐
6.3.4	Ensure Prevent Cross-site Tracking in Safari Is Enabled	☐	☐
6.3.5	Audit Hide IP Address in Safari Setting	☐	☐
6.3.6	Ensure Advertising Privacy Protection in Safari Is Enabled	☐	☐
6.3.7	Ensure Show Full Website Address in Safari Is Enabled	☐	☐
6.3.8	Audit AutoFill	☐	☐
6.3.9	Audit Pop-up Windows	☐	☐
6.3.10	Ensure Show Status Bar Is Enabled	☐	☐
6.4.1	Ensure Secure Keyboard Entry Terminal.app Is Enabled	☐	☐
6.5.1	Audit Passwords	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure Apple-provided Software Updates Are Installed	☐	☐
1.2	Ensure Download New Updates When Available Is Enabled	☐	☐
1.3	Ensure Install of macOS Updates Is Enabled	☐	☐
1.4	Ensure Install Application Updates from the App Store Is Enabled	☐	☐
1.5	Ensure Install Security Responses and System Files Is Enabled	☐	☐
1.6	Ensure Software Update Deferment Is Less Than or Equal to 30 Days	☐	☐
2.1.1.1	Audit iCloud Passwords & Keychain	☐	☐
2.1.1.2	Audit iCloud Drive	☐	☐
2.1.1.3	Ensure iCloud Drive Document and Desktop Sync Is Disabled	☐	☐
2.1.1.4	Audit Security Keys Used With Apple Accounts	☐	☐
2.1.1.5	Audit Freeform Sync to iCloud	☐	☐
2.1.1.6	Audit Find My Mac	☐	☐
2.1.2	Audit App Store Password Settings	☐	☐
2.2.1	Ensure Firewall Is Enabled	☐	☐
2.2.2	Ensure Firewall Stealth Mode Is Enabled	☐	☐
2.3.1.1	Ensure AirDrop Is Disabled When Not Actively Transferring Files	☐	☐
2.3.1.2	Ensure AirPlay Receiver Is Disabled	☐	☐
2.3.2.1	Ensure Set Time and Date Automatically Is Enabled	☐	☐
2.3.2.2	Ensure the Time Service Is Enabled	☐	☐
2.3.3.1	Ensure Screen Sharing Is Disabled	☐	☐
2.3.3.2	Ensure File Sharing Is Disabled	☐	☐
2.3.3.3	Ensure Printer Sharing Is Disabled	☐	☐
2.3.3.4	Ensure Remote Login Is Disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.3.3.5	Ensure Remote Management Is Disabled	☐	☐
2.3.3.6	Ensure Remote Apple Events Is Disabled	☐	☐
2.3.3.7	Ensure Internet Sharing Is Disabled	☐	☐
2.3.3.8	Ensure Content Caching Is Disabled	☐	☐
2.3.3.9	Ensure Media Sharing Is Disabled	☐	☐
2.3.3.10	Ensure Bluetooth Sharing Is Disabled	☐	☐
2.3.3.11	Ensure Computer Name Does Not Contain PII or Protected Organizational Information	☐	☐
2.3.4.1	Ensure Backup Automatically is Enabled If Time Machine Is Enabled	☐	☐
2.3.4.2	Ensure Time Machine Volumes Are Encrypted If Time Machine Is Enabled	☐	☐
2.4.1	Audit Menu Bar and Control Center Icons	☐	☐
2.5.1.1	Ensure External Intelligence Extensions Is Disabled	☐	☐
2.5.1.2	Ensure Writing Tools Is Disabled	☐	☐
2.5.1.3	Ensure Mail Summarization Is Disabled	☐	☐
2.5.1.4	Ensure Notes Summarization Is Disabled	☐	☐
2.5.2.1	Ensure Siri Is Disabled	☐	☐
2.5.2.2	Ensure Listen for (Siri) Is Disabled	☐	☐
2.6.1.1	Ensure Location Services Is Enabled	☐	☐
2.6.1.2	Ensure 'Show Location Icon in Control Center when System Services Request Your Location' Is Enabled	☐	☐
2.6.1.3	Audit Location Services Access	☐	☐
2.6.2.1	Audit Full Disk Access for Applications	☐	☐
2.6.3.1	Ensure Share Mac Analytics Is Disabled	☐	☐
2.6.3.2	Ensure Improve Siri & Dictation Is Disabled	☐	☐
2.6.3.3	Ensure Improve Assistive Voice Features Is Disabled	☐	☐
2.6.3.4	Ensure 'Share with app developers' Is Disabled	☐	☐
2.6.3.5	Ensure Share iCloud Analytics Is Disabled	☐	☐
2.6.4	Ensure Limit Ad Tracking Is Enabled	☐	☐
2.6.5	Ensure Gatekeeper Is Enabled	☐	☐
2.6.6	Ensure FileVault Is Enabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.6.7	Audit Lockdown Mode	☐	☐
2.6.8	Ensure an Administrator Password Is Required to Access System-Wide Preferences	☐	☐
2.7.1	Ensure Screen Saver Corners Are Secure	☐	☐
2.8.1	Audit Universal Control Settings	☐	☐
2.9.1	Ensure Help Apple Improve Search Is Disabled	☐	☐
2.10.1.1	Ensure the OS Is Not Active When Resuming from Standby (Intel)	☐	☐
2.10.1.2	Ensure Sleep and Display Sleep Is Enabled on Apple Silicon Devices	☐	☐
2.10.2	Ensure Power Nap Is Disabled for Intel Macs	☐	☐
2.10.3	Ensure Wake for Network Access Is Disabled	☐	☐
2.11.1	Ensure an Inactivity Interval of 15 Minutes Or Less for the Screen Saver Is Enabled	☐	☐
2.11.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	☐	☐
2.11.3	Ensure a Custom Message for the Login Screen Is Enabled	☐	☐
2.11.4	Ensure Login Window Displays as Name and Password Is Enabled	☐	☐
2.11.5	Ensure Show Password Hints Is Disabled	☐	☐
2.12.1	Ensure Users' Accounts Do Not Have a Password Hint	☐	☐
2.12.2	Audit Touch ID	☐	☐
2.13.1	Ensure Guest Account Is Disabled	☐	☐
2.13.2	Ensure Guest Access to Shared Folders Is Disabled	☐	☐
2.13.3	Ensure Automatic Login Is Disabled	☐	☐
2.15.1	Audit Notification Settings	☐	☐
2.17.1	Audit Internet Accounts for Authorized Use	☐	☐
2.18.1	Ensure On-Device Dictation Is Enabled	☐	☐
3.1	Ensure Security Auditing Is Enabled	☐	☐
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	☐	☐
3.4	Ensure Security Auditing Retention Is Enabled	☐	☐
3.5	Ensure Access to Audit Records Is Controlled	☐	☐
3.6	Audit Software Inventory	☐	☐
4.1	Ensure Bonjour Advertising Services Is Disabled	☐	☐
4.2	Ensure HTTP Server Is Disabled	☐	☐
4.3	Ensure NFS Server Is Disabled	☐	☐
5.1.1	Ensure Home Folders Are Secure	☐	☐
5.1.2	Ensure System Integrity Protection Status (SIP) Is Enabled	☐	☐
5.1.3	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	☐	☐
5.1.4	Ensure Signed System Volume (SSV) Is Enabled	☐	☐
5.1.5	Ensure Appropriate Permissions Are Enabled for System Wide Applications	☐	☐
5.1.6	Ensure No World Writable Folders Exist in the System Folder	☐	☐
5.1.7	Ensure No World Writable Folders Exist in the Library Folder	☐	☐
5.2.1	Ensure Password Account Lockout Threshold Is Configured	☐	☐
5.2.2	Ensure Password Minimum Length Is Configured	☐	☐
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	☐	☐
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	☐	☐
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	☐	☐
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	☐	☐
5.2.7	Ensure Password Age Is Configured	☐	☐
5.2.8	Ensure Password History Is Set to at least 24	☐	☐
5.3.1	Ensure all user storage APFS volumes are encrypted	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.3.2	Ensure all user storage CoreStorage volumes are encrypted	☐	☐
5.4	Ensure the Sudo Timeout Period Is Set to Zero	☐	☐
5.5	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	☐	☐
5.6	Ensure the "root" Account Is Disabled	☐	☐
5.7	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	☐	☐
5.8	Ensure a Login Window Banner Exists	☐	☐
5.9	Ensure the Guest Home Folder Does Not Exist	☐	☐
5.10	Ensure XProtect Is Running and Updated	☐	☐
5.11	Ensure Logging Is Enabled for Sudo	☐	☐
6.1.1	Audit Show All Filename Extensions	☐	☐
6.2.1	Ensure Protect Mail Activity in Mail Is Enabled	☐	☐
6.3.1	Ensure Automatic Opening of Safe Files in Safari Is Disabled	☐	☐
6.3.2	Audit History and Remove History Items	☐	☐
6.3.3	Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled	☐	☐
6.3.4	Ensure Prevent Cross-site Tracking in Safari Is Enabled	☐	☐
6.3.5	Audit Hide IP Address in Safari Setting	☐	☐
6.3.6	Ensure Advertising Privacy Protection in Safari Is Enabled	☐	☐
6.3.7	Ensure Show Full Website Address in Safari Is Enabled	☐	☐
6.3.8	Audit AutoFill	☐	☐
6.3.9	Audit Pop-up Windows	☐	☐
6.3.10	Ensure Show Status Bar Is Enabled	☐	☐
6.4.1	Ensure Secure Keyboard Entry Terminal.app Is Enabled	☐	☐
6.5.1	Audit Passwords	☐	☐

Internal Only - General

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	☐	☐

Internal Only - General

Appendix: Change History

Date	Version	Changes for this version
Oct 17, 2025	1.0.0	Initial Draft Release
Oct 31, 2025	1.0.0	Initial Benchmark Release

Internal Only - General